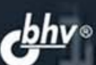
Д. Колисниченко



БЕЗОПАСНЫЙ ANDROID: ЗАЩИЩАЕМ СВОИ ДЕНЬГИ И ДАННЫЕ ОТ КРАЖИ

- Шифрование данных, хранящихся на Android-устройстве
- Шифрование передаваемых данных
- VPN-соединения
- Анонимизация трафика с помощью Tor
- Ограничение запуска приложений
- Антивирусы и брандмауэры
- Поиск потерянного или украденного устройства
- Вопросы семейной безопасности
- Экономия трафика, защита от спама
- Получение прав root





Денис Колисниченко

БЕЗОПАСНЫЙ ANDROID: ЗАЩИЩАЕМ СВОИ ДЕНЬГИ И ДАННЫЕ ОТ КРАЖИ

Санкт-Петербург
«БХВ-Петербург»
2015

УДК 004.4
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

К60 Безопасный Android: защищаем свои деньги и данные от кражи. — СПб.: БХВ-Петербург, 2015. — 161 с.: ил.

ISBN 978-5-9775-3149-8

Рассмотрены различные способы обеспечения безопасности Android-устройств: шифрование персональной информации, хранящейся на устройстве, шифрование передаваемых данных, VPN-соединения, анонимизация трафика, выбор и использование антивируса и брандмауэра, поиск потерянного или украденного устройства, экономия трафика, защита от спама, получение прав root. Уделено внимание вопросам личной и семейной безопасности (ограничение доступа ребенка к определенным ресурсам/программам, отслеживание телефона ребенка и т. д.). Практически все рассмотренное в книге программное обеспечение бесплатное, что поможет не только защитить ваше устройство, но и сэкономить деньги.

Для широкого круга пользователей Android

УДК 004.4
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Григорий Добин*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Марины Дамбиевой*

Подписано в печать 30.01.15.
Формат 70×100 $^{1}/_{16}$. Печать офсетная. Усл. печ. л. 12,9.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3149-8

Оглавление

Введение

Современные мобильные телефоны (смартфоны) уже давно перестали быть просто телефонами. По сути, у каждого из нас в кармане находится мини-компьютер, способный на многое. Установленное на нем стандартное программное обеспечение позволяет просматривать интернет-сайты, получать и отправлять электронную почту, обмениваться файлами, открывать документы популярных офисных пакетов, читать электронные книги, слушать музыку и смотреть фильмы. И это уже не говоря о дополнительном программном обеспечении, которое можно установить абсолютно бесплатно или за символическую плату.

Мобильный телефон, ставший смартфоном, постепенно превратился в средство хранения и обработки персональной информации: через него вы можете вести деловую или личную переписку по электронной почте, общаться в Skype и других подобных программах, хранить на SD-карте телефона конфиденциальную (и даже платежную) информацию — никто не запрещает оплачивать со своего банковского счета покупки, используя для этого смартфон.

Но всю свою персональную информацию нужно защищать — от вирусов и вредоносных программ, которые могут похитить ту самую платежную информацию и прочие пароли и использовать это вам в ущерб, а также и от недоброжелателей, которым тем или иным путем попал в руки ваш мобильный телефон.

Эта книга посвящена обеспечению безопасности мобильных устройств на базе операционной системы Android. Защитить свой телефон, а значит, и свои данные, а вместе с ними и свою нервную систему, может каждый. Как вы заметите, большинство программ обеспечения безопасности просты в установке и использовании.

В книге нет никакой «высшей математики», так что освоить приведенный в ней материал может даже школьник (разве что за исключением *глав 10* и *11*, где подразумевается наличие у читателя некоторых специальных знаний).

Организация книги

Книга состоит из 11 глав и одного приложения. Из *главы 1* вы узнаете, что ***не*** следует делать, чтобы не превратить ваш смартфон в бесполезное устройство, или, попросту, «кирпич». Вы думаете, я шучу? У меня уже есть смартфон, оживить который сможет разве что чудо. И я не один такой. Может, когда найду для этого

время, то еще раз попытаюсь его реанимировать, но глубоко сомневаюсь, что получится.

В *главе 2* приводятся общие рекомендации, позволяющие сохранить ваши данные в целости и сохранности.

Глава 3 более практическая, и в ней мы избавимся от повышенного расхода трафика — беды всех Android-устройств. Помочь в этой ситуации можно двумя способами: или перейти на тариф с безлимитным доступом к Интернету, или же следовать рекомендациям *главы 3* и избавиться от этой проблемы раз и навсегда. Ну, почти навсегда...

Если в *главе 3* мы защищали карман, то в *главе 4* речь пойдет о защите персональных данных, а именно — о шифровании отдельных файлов и всего устройства.

Android — довольно-таки безопасная операционная система. Нужен ли для Android антивирус? Ответ на этот вопрос вы узнаете из *главы 5*, в ней также пойдет речь о выборе подходящего антивируса.

Мы защитили хранящиеся на смартфоне данные от злоумышленников и кражи. Но как защитить передаваемые данные? В этом вам поможет шифрование интернет-соединения, а о том, как его настроить, рассказано в *главе 6*.

Надеюсь, вы никогда не потеряете свой смартфон, и у вас его никто не украдет. Однако если такое произошло, помочь найти потерянное/украденное устройство поможет *глава 7*.

Глава 8 посвящена личной безопасности, а в *главе 9* рассматриваются различные системные приемы — например, вы узнаете, как избавиться от надоедливой рекламы, как установить файловый менеджер, как восстановить удаленные файлы и т. п.

Глава 10 посвящена получению прав пользователя root. Сразу хочется отметить, что в процессе этой процедуры легко превратить свой смартфон в «кирпич», так что будьте осторожны.

Но еще более осторожным нужно быть, следуя рекомендациям *главы 11*, когда мы попытаемся установить на один смартфон две операционные системы Android. Если вы сомневаетесь в своих знаниях и умениях, лучше прочитать *главу 11* только для «общего развития», но не пытаться ничего воспроизвести.

Для Android разработано очень, очень много приложений. Трудно даже представить себе, сколько их существует и предлагается для установки. В этой книге, чтобы не запутать читателя, я старался рассматривать для каждой цели только одно какое-либо приложение. Программы тщательно отбирались — в книге представлены только те приложения, которые я использую сам и которые в настоящий момент установлены на моих устройствах. Но никогда не будет лишним взглянуть и на альтернативное программное обеспечение. Может, вам что-то подойдет больше. Именно поэтому настоятельно рекомендую ознакомиться с *приложением*, в котором описаны дополнительные программы, также способные обеспечить безопасность вашему смартфону.

Не смею вас больше задерживать — самое время приступить к чтению книги!



ГЛАВА 1

Как не превратить свой смартфон в «кирпич»?

1.1. Немного об эволюции мобильного телефона

Современный мобильный телефон уже давно превратился в небольшой персональный компьютер с полноценной операционной системой. Еще десять лет назад сломать мобильный телефон можно было лишь физически: разбить, утопить или совершить прочие подобные акты вандализма по отношению к довольно-таки полезному устройству. За эти десять лет многое изменилось, поменялось даже название самого мобильного телефона — теперь их называют *смартфонами*, чтобы подчеркнуть, что это не просто мобильный телефон, а устройство с дополнительными «умными» (smart) функциями.

Итак, во-первых, *унифицировано системное программное обеспечение*. Да, десять лет назад на мобильные устройства также можно было устанавливать приложения. Речь здесь, конечно, не идет о совсем уж «древних» аппаратах конца 1990-х — начала 2000-х годов. Эти динозавры нужно было «перепрошивать» даже для простого изменения мелодии, не говоря уже об установке программ. Но на более «современные» телефоны прошлого десятилетия уже можно было устанавливать дополнительное программное обеспечение. Однако и здесь не все было так просто — программное обеспечение разных производителей, как правило, оказывалось не совместимым между собой. Например, вы не могли скачать программу для Siemens и установить ее на Nokia. Более того, несовместимым часто могло быть программное обеспечение, написанное для разных моделей одного и того же производителя. Такая ситуация напрочь отбивала желание вообще что-либо устанавливать. Даже если какую-нибудь программу (а их было не так уж и много) и удавалось установить, то это событие отмечалось как маленькая победа.

Но вот, в 2008 году, свершилось чудо — была разработана ОС Android. Эта операционная система обеспечила столь необходимую универсальность, и теперь вы можете устанавливать (и удалять) Android-программы на любой смартфон, работающий под управлением Android, хоть по нескольку раз на дню: установил — не понравилось — удалил. Никаких ограничений нет (если не считать того, что неко-

торые приложения — коммерческие). Казалось бы, вот оно счастье! Но не тут-то было. Свобода несет в себе и некую опасность. Пользователь, например, может установить вредоносную программу, замаскированную под необходимый для него программный продукт. Взять тот же навигатор Navitel — это коммерческая программа, и пользователь может использовать ее бесплатно лишь 30 дней, после чего нужно купить ключ. Некоторым несознательным пользователям покупать ничего не хочется, поэтому они устанавливают Navitel из непроверенного источника и вместе с навигатором получают «троянского коня». Что будет делать этот «конь», зависит только от фантазии его разработчиков. Он может, например, обеспечивая функционирование навигации (т. е. Navitel все-таки будет в комплекте), записывать и пересылать третьей стороне все телефонные разговоры, SMS, фотографии и другие ваши конфиденциальные данные. А может просто взять и удалить все пользовательские данные с карты памяти устройства. Особо «злые» программы могут даже уничтожить ваш смартфон, превратив его в «кирпич».

Во-вторых, *изменилась функциональность устройства*. Теперь оно «напичкано» всевозможными датчиками. Если раньше телефон имел только динамик, микрофон и, может быть, веб-камеру весьма сомнительного качества, то сейчас не хватает, наверное, лишь датчика дождя. Все остальное в ваш смартфон уже встроено. К счастью, наличие этих датчиков (сенсоров) никак не может повредить непосредственно устройство, но представляет собой в некотором роде проблему для самого его владельца. Так, ориентируясь на GPS-модуль устройства, можно отследить его перемещение на местности. Конечно, оператор мобильной сети и так может следить за перемещениями пользователя, даже если у него обычный телефон десятилетней давности. Но здесь речь идет о том, что любой желающий, завладевший вашим телефоном всего на несколько минут (например, когда вы в офисе забыли его на столе, или просто попросивший его у вас, чтобы якобы поговорить по телефону, поскольку его собственный телефон разрядился), может установить некое приложение, которое будет следить за всеми вашими перемещениями и сообщать о них, куда надо. Согласитесь, это не очень хорошо. Точно так же существуют приложения, которые постоянно или по команде извне могут начать запись и трансляцию в нужном направлении всего, что происходит в данный момент вокруг устройства — т. е. ваш смартфон будет использоваться как обычный «жучок». И поверьте, не нужно быть семи пядей во лбу, чтобы разработать такие приложения.

В-третьих, теперь, кроме списка SMS, адресной книги и перечня последних набранных номеров, *в смартфоне хранится серьезная личная информация*. Возможности Android позволяют устанавливать на смартфоны и планшеты обычные офисные приложения, а это означает, что в памяти вашего мобильного устройства могут содержаться важные документы, конфиденциальная переписка по электронной почте, личные фотографии и прочие данные, которые могут использовать против вас конкуренты или «доброжелатели». Всю такую информацию нужно защищать. И сегодня это не проблема, поскольку на современных смартфонах установлены мощные многоядерные процессоры, для которых шифрование — по зубам. В *главе 4* мы как раз и рассмотрим способы защиты ваших персональных данных. Но если этот вопрос беспокоит вас больше прочих, вы можете перейти к ее чтению прямо сейчас, а затем уже дочитать пропущенные главы.

1.2. Меры предосторожности

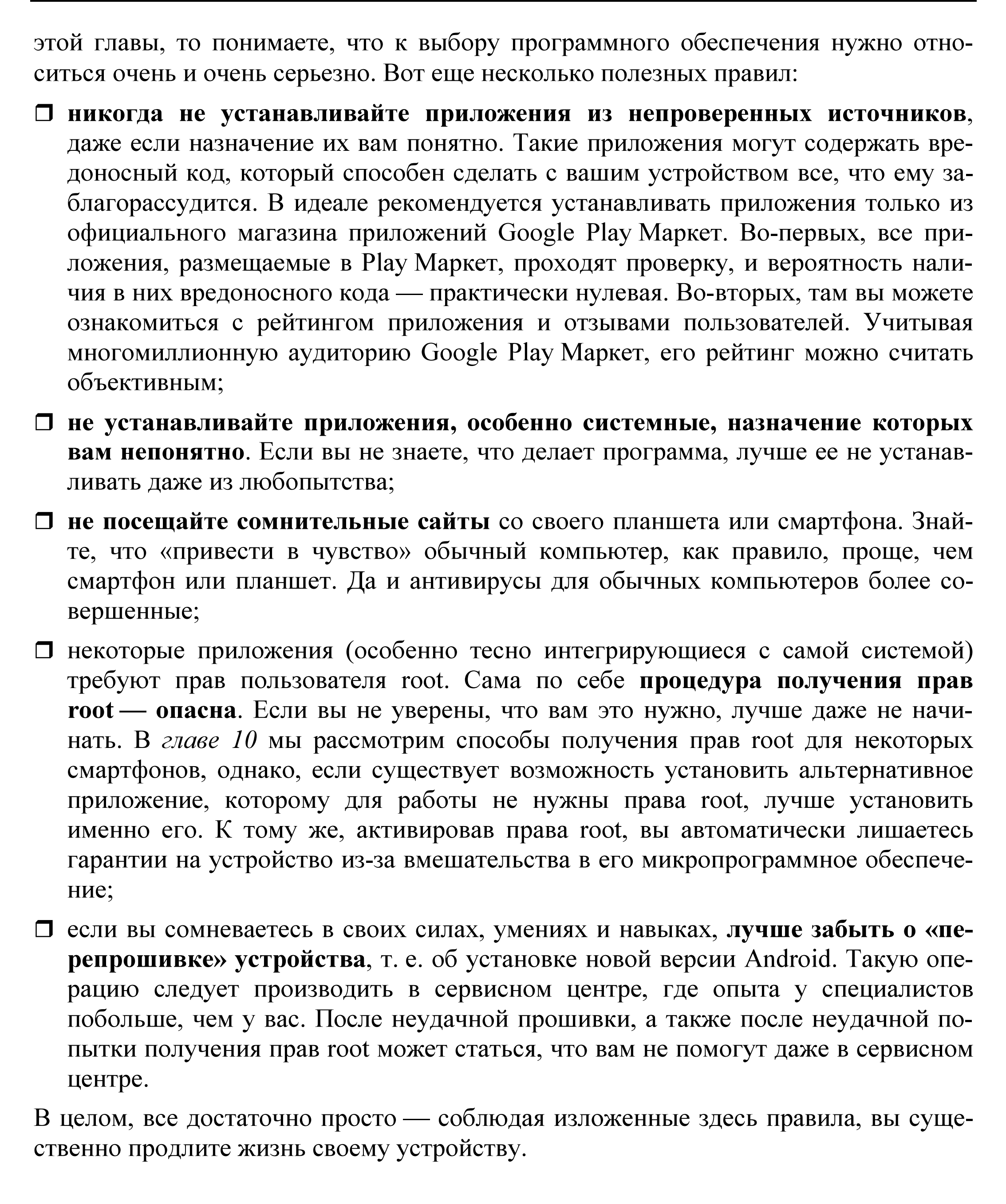
Теперь поговорим о том, как не испортить ваш ~~мобильный телефон~~, ой, смартфон. Начнем с мер физической предосторожности. Все-таки смартфон — сложное и относительно дорогое устройство, и хочется, чтобы оно работало долго и безотказно. Все мы люди адекватные и прекрасно понимаем, что бросать смартфон об стену, пытаться утопить его или бить по нему молотком — не сто́ит. Конечно, существуют специальные защищенные модели, выпускаемые компаниями Sigma и Tetex, они предназначены для экстремального использования, однако большинство устройств не выдержит и половины того, что могут выдержать защищенные аппараты.

Вот несколько советов, следование которым позволит сохранить смартфон или планшет в целости и сохранности хотя бы физически:

- **купите защитный чехол** — он не только убережет устройство от царапин, но и существенно повысит шансы его выживания при падении. Чехол также удобен и тем, что при падении смартфон не рассыплется на несколько частей: заднюю крышку, аккумулятор и т. п.;
- **старайтесь не говорить под дождем** — полагаю, не нужно рассказывать, почему влага это плохо. Опять-таки, от небольшого дождя спасет чехол;
- **остерегайтесь перепада температур**. Одним не очень прекрасным утром я обнаружил, что сенсорный дисплей моего смартфона не работает, хотя вечером все было прекрасно. Вердикт сервисной службы гласил — попала влага. И поскольку под дождь я с ним не попадал и под краном его не мыл, видимо, виной всему оказался конденсат. Отделался я легким испугом — смартфон полежал в разобранном состоянии несколько дней, а когда его собрали, то он заработал, хотя изначально предлагалось поменять сенсорный экран — хорошо что в сервисе его не было в наличии, а доставка затянулась.

  Итак, когда вы выходите из теплого помещения на мороз, не нужно сразу вытаскивать смартфон, пусть он полежит с полчаса в кармане и постепенно остынет. Карман сыграет роль «термоса». Аналогично, когда вы заходите с мороза в теплое помещение, не следует без крайней необходимости пользоваться смартфоном — пусть он те же полчаса полежит в кармане или сумке. По себе знаю, придерживаться этого совета очень сложно, но мое дело рассказать, а ваше — сделать выводы... и продолжать использовать смартфон как обычно;
- **у планшета должен быть свой «дом»** — найдите место, например, на столе возле ноутбука, где планшет должен находиться всегда, когда вы его не используете. Если бросать планшет где угодно, на него элементарно можно сесть, наступить и т. п. То же самое касается и смартфона, хотя придерживаться этого правила весьма трудно. Пишу эти строки, а сам пытаюсь вспомнить, где же мой смартфон...

Физические меры предосторожности — это хорошо, но чаще смартфоны и планшеты приходят в негодность не из-за физического воздействия, а вследствие неправильных действий пользователя. Если вы внимательно прочитали первый раздел



этой главы, то понимаете, что к выбору программного обеспечения нужно относиться очень и очень серьезно. Вот еще несколько полезных правил:

- **никогда не устанавливайте приложения из непроверенных источников**, даже если назначение их вам понятно. Такие приложения могут содержать вредоносный код, который способен сделать с вашим устройством все, что ему заблагорассудится. В идеале рекомендуется устанавливать приложения только из официального магазина приложений Google Play Маркет. Во-первых, все приложения, размещаемые в Play Маркет, проходят проверку, и вероятность наличия в них вредоносного кода — практически нулевая. Во-вторых, там вы можете ознакомиться с рейтингом приложения и отзывами пользователей. Учитывая многомиллионную аудиторию Google Play Маркет, его рейтинг можно считать объективным;
- **не устанавливайте приложения, особенно системные, назначение которых вам непонятно**. Если вы не знаете, что делает программа, лучше ее не устанавливать даже из любопытства;
- **не посещайте сомнительные сайты** со своего планшета или смартфона. Знайте, что «привести в чувство» обычный компьютер, как правило, проще, чем смартфон или планшет. Да и антивирусы для обычных компьютеров более совершенные;
- некоторые приложения (особенно тесно интегрирующиеся с самой системой) требуют прав пользователя root. Сама по себе **процедура получения прав root — опасна**. Если вы не уверены, что вам это нужно, лучше даже не начинать. В *главе 10* мы рассмотрим способы получения прав root для некоторых смартфонов, однако, если существует возможность установить альтернативное приложение, которому для работы не нужны права root, лучше установить именно его. К тому же, активировав права root, вы автоматически лишаетесь гарантии на устройство из-за вмешательства в его микропрограммное обеспечение;
- если вы сомневаетесь в своих силах, умениях и навыках, **лучше забыть о «перепрошивке» устройства**, т. е. об установке новой версии Android. Такую операцию следует производить в сервисном центре, где опыта у специалистов побольше, чем у вас. После неудачной прошивки, а также после неудачной попытки получения прав root может статься, что вам не помогут даже в сервисном центре.

В целом, все достаточно просто — соблюдая изложенные здесь правила, вы существенно продлите жизнь своему устройству.



ГЛАВА 2

Общая безопасность Android-устройства

В предыдущей главе мы поговорили о том, чего *не следует делать*, чтобы не превратить свое дорогое и современное устройство в никому не нужный «кирпич». Здесь же мы посмотрим на проблему с другой стороны, а именно — поговорим о том, что *нужно делать*, чтобы обезопасить свои данные, свое устройство и себя.

Далее приведено несколько простых рекомендаций. Позже, в последующих главах, каждая из рекомендаций будет рассмотрена подробно.

2.1. Отказ от установки приложений из неизвестных источников

Очень часто причиной всех несчастий для владельцев Android-устройства является установка вредоносной программы. Чтобы исключить хотя бы неявную или случайную установку такой программы, рекомендуется запретить установку программ из неизвестных источников.

Безопасным источником считается только Google Play Маркет — по сути, так оно и есть. В этом смысле, например, ваша SD-карта — тоже неизвестный источник, поэтому просто так установить APK-файл, присланный приятелем, уже не получится. Зато вы предотвратите потенциальную угрозу.

Для отключения установки из неизвестных источников перейдите в меню **Настройки | Безопасность** и *выключите* (снимите соответствующую птичку) параметр **Неизвестные источники** (рис. 2.1).

Чтобы вновь получить возможность устанавливать APK-файлы, полученные извне, включите этот параметр для конкретной установки. По крайней мере, вы установите данные APK-файлы осознанно. Думаю, не стоит говорить, что для большей безопасности после установки требуемых APK-файлов параметр **Неизвестные источники** следует выключить снова.

Рекомендуется также включить параметр **Проверять приложения** — система тогда будет блокировать запуск потенциально опасных приложений. Жаль, что этот параметр появился в Android, только начиная с версии 4.1, и его не было в предыдущих версиях.

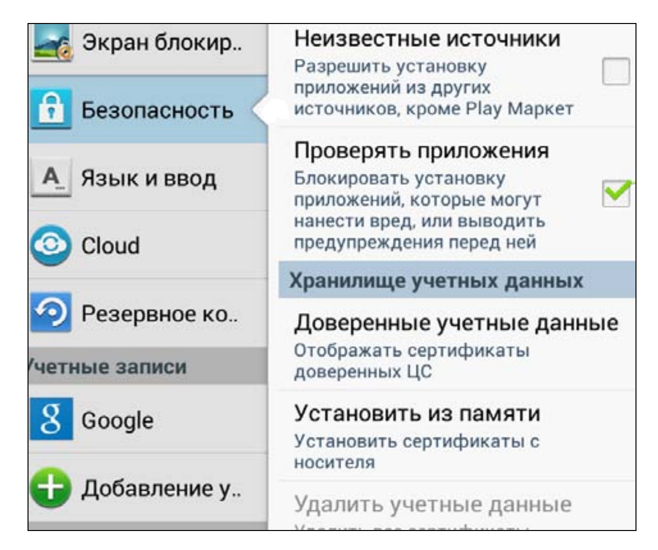


Рис. 2.1. Отключение установки из неизвестных источников

2.2. Осторожно: неизвестные сети Wi-Fi!

Не подключайтесь к неизвестным сетям Wi-Fi, особенно к публичным, происхождение которых вам неизвестно. Может быть, кто-то просто не смог правильно настроить маршрутизатор Wi-Fi, не установил на нем соответствующий пароль, и теперь к его сети может получить доступ любой желающий, и вы в том числе. А может, такая сеть развернута злоумышленниками преднамеренно, чтобы перехватывать все передающиеся по ней данные, в том числе и конфиденциальные, такие как пароли и номера кредитных карточек, и сопутствующую финансовую информацию.

Вообще, с осторожностью относитесь к публичным сетям (аэропорта, ресторана, отеля и т. п.). Никогда нельзя знать, как они настроены. Если приходится передавать данные по таким сетям, шифруйте передаваемые данные. О защите передаваемых по сети данных мы поговорим в *главе 6*. Из нее вы также узнаете, как скрыть свой IP-адрес и получить хоть какую-то анонимность.

Способы шифрования передаваемых данных

Забегая вперед, отмечу, что существуют два способа шифрования передаваемых данных, доступных в Android. Первый заключается в организации VPN-соединения (от англ. ***V****irtual* ***P****rivate* ***N****etwork* — виртуальная частная сеть), второй — в использовании Tor (от англ. ***T****he* ***O****nion* ***R****outer* — системы так называемой «луковой маршрутизации», создающей каскад из прокси-серверов, что позволяет устанавливать анонимное сетевое соединение, защищенное от прослушивания). Первый способ удобнее тем, что будет зашифрован весь интернет-трафик всех приложений. Но VPN-сервисы обычно платные, т. е. за VPN-трафик придется заплатить. Впрочем, некоторые сервисы предоставляют 100–150 Мбайт бесплатного трафика, чтобы вы могли протестировать скорость и надежность VPN-соединения, чем иногда удается воспользоваться. А вот система Tor бесплатна полностью, вот только не всегда скорость работы через нее соответствует вашим ожиданиям. Кроме того, если вы не получили на своем смарт-

фоне права root (см. об этом в *главе 10*), то через Tor будут работать не все приложения, а только те, которые поддерживают Orbot (официальную версию Tor-клиента для Android). Надеюсь, я вас заинтересовал, и теперь вы не пропустите *главу 6* ☺.

2.3. Установка антивируса

Чтобы обеспечить безопасность самого устройства, установите антивирус. К сожалению, Android тоже может «подхватывать» вирусы. Конечно, «вирусы для Android» — это громко сказано, и в таком понимании, в котором они существуют для Windows, в Android их нет хотя бы потому, что в 99 процентах случаев пользователю не предоставлены root-права, и вирус даже при всем своем желании не может натворить ничего такого, что могло бы причинить вред самой Android. А оставшийся один процент — это пользователи, которые сами получили root-доступ. Пусть теперь пеняют на себя.

В мире Android вирусы — это программы-нарушители, но от этого не легче. Например, такая программа может подслушать вас, отправить SMS на платный номер, украсть ваши личные данные — например, Google-аккаунт или приватные фотографии и т. п. К тому же, вы можете обмениваться файлами, например, документами MS Office, содержащими вирусы. Вот все такие попытки и должен пресечь Android-антивирус.

Самой Android такие вирусы, скорее всего, не навредят, но инфицированные файлы, переданные вами на Windows-компьютеры, могут там причинить вред. О выборе антивируса мы поговорим в *главе 5*. Из нее вы узнаете, какой антивирус лучше, а также ознакомитесь с общими рекомендациями, позволяющими исключить вероятность заражения смартфона.

2.4. Включение шифрования и использование других средств защиты данных

Для защиты личных данных — например, важных документов, фотографий — одного графического пароля или пинкода мало. Если ваше устройство (смартфон, планшет) попадет в руки злоумышленников, то знайте — избавиться от графического пароля очень просто (см. об этом в *главе 10*). Да проще простого извлечь из смартфона карту памяти и прочитать ее на другом устройстве (например, на ноутбуке). Поэтому важные данные можно и нужно шифровать. Шифрованию данных посвящена *глава 4* этой книги.

Для защиты личных данных можно использовать и другие средства — например, программы, скрывающие папки и запрещающие запуск определенных приложений. Может быть, толку от них и не много, но эти средства все же лучше, чем ничего. В частности, они помогут скрыть важные данные от любопытных коллег, когда вы забудете телефон на столе и ненадолго отойдете.

Android-устройство можно в некоторой степени использовать и для обеспечения собственной безопасности. Например, с помощью специальных программ превратить смартфон в «тревожную кнопку», в небольшую систему видеонаблюдения и в диктофон, позволяющий записывать не только происходящее вокруг, но и ваши телефонные разговоры. Все эти вопросы будут рассмотрены в *главе 9*.

2.5. Отключение GPS-модуля

Во избежание отслеживания вашего передвижения (некоторые вредоносные программы могут передавать ваши GPS-координаты третьей стороне) отключите GPS-модуль, когда вы ним не пользуетесь. Конечно, есть и моменты, когда GPS необходим. В этом случае придется определить, какая программа (кроме программы навигации) обращается к демону `gpsd`.

Отключение GPS-модуля также поможет сэкономить заряд аккумулятора. Именно поэтому я рекомендую всегда отключать GPS, когда он вам не нужен. Лично мой планшет с включенным GPS-модулем значительно быстрее разряжается (а при запущенной программе навигации его вообще хватает на 3 часа).

Для отключения GPS и вообще функции определения вашего местоположения перейдите в меню **Настройки | Местоположение** и выключите параметры **Использовать GPS**, **Беспроводные сети** и **Доступ к данным о моем местоположении** (на рис. 2.2 все эти параметры как раз включены).

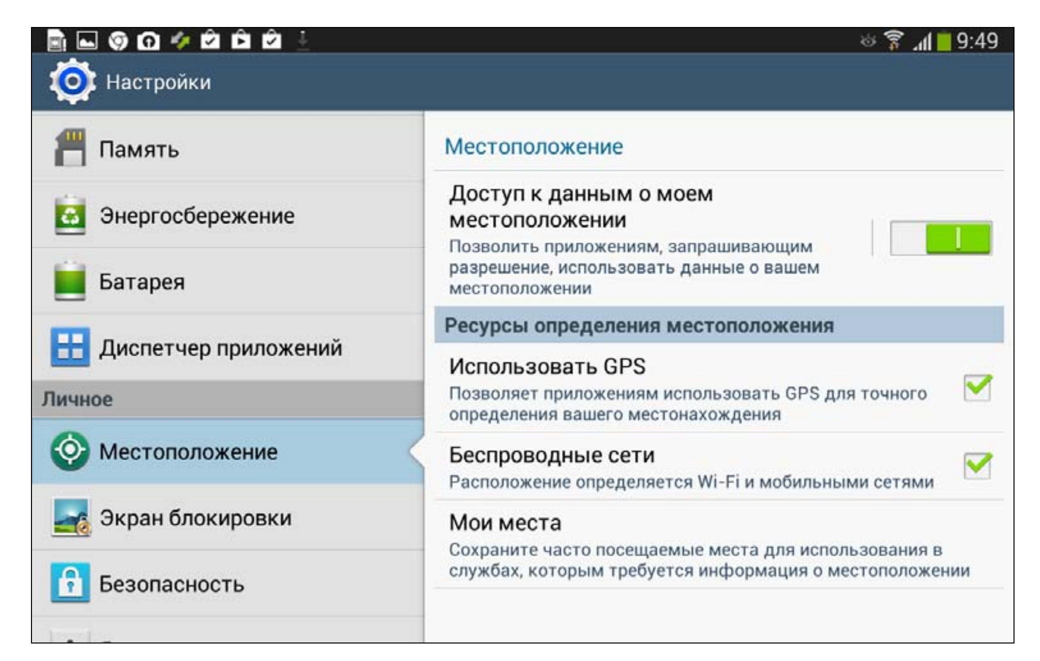


Рис. 2.2. Отключение определения местоположения

Помните, что отключение этих параметров всего лишь не позволит программам получать доступ к данным о вашем местоположении. Если вы не хотите, чтобы оператор сети знал[1], где вы находитесь, выключите устройство и извлеките из него аккумулятор. Кнопка выключения — это не аппаратное выключение, когда физически размыкаются контакты, а всего лишь так называемый *soft-off* — т. е. теоретически устройство все еще может принимать и передавать данные. Гарантировать, что произошло полное отключение устройства может лишь извлечение аккумулятора. При этом аккумулятор легко извлекается из большинства смартфонов, однако аккумуляторы планшетов в большинстве случаев извлечь нельзя, к сожалению.

[1] Может ли оператор установить местоположение выключенного телефона? Ответ на этот вопрос читайте по адресу: **http://habrahabr.ru/post/112449/**.



ГЛАВА 3

Как избавиться от повышенного расхода трафика?

3.1. Куда девается трафик?

Начнем эту главу с рассмотрения весьма беспокоящего момента — расхода трафика. До знакомства с Android я не мог ответить на два вопроса: откуда берется пыль и куда деваются деньги? Сейчас к списку интересующих меня вопросов добавился еще один: куда девается трафик?

Перерасход трафика особенно заметен пользователям, которые перешли на Android с устройств с системами Bada и Symbian на борту. Конечно, самый удобный способ забыть об этой проблеме — купить пакет с безлимитным Интернетом. Однако это не всегда имеет смысл, поскольку у так называемых «безлимитных» пакетов нередко не совсем приличные тарифы на обычные телефонные звонки. Поэтому особой выгоды добиться так не получится: если Интернет будет дешевым, а обычные звонки — нет. Купить еще одну SIM-карту и использовать ее, когда нужно работать в Интернете, — тоже не всегда выход, т. к. в этом случае вы не сможете воспользоваться интернет-виджетами (тем же прогнозом погоды) — т. е. включить-то их будет можно, но на обычной SIM-карте интернет-тариф вам не понравится.

3.2. Аппаратное решение

Для разрешения ситуации можно предложить сугубо аппаратное решение. Все смартфоны умеют подключаться к Интернету по Wi-Fi, поэтому достаточно купить мобильный маршрутизатор (роутер) Wi-Fi, установить в него SIM-карту с самым дешевым доступом к Интернету и получить Интернет на смартфон от роутера по Wi-Fi (при этом совсем не обязательно, чтобы оператор этой сети совпадал с вашим основным). Получается, что в вашем смартфоне стоит SIM-карта оператора, тарифы на телефонные звонки которого вас устраивают больше всего, а в маршрутизаторе установлена SIM-карта оператора, у которого самый дешевый Интернет.

Мобильный маршрутизатор Wi-Fi — весьма компактное устройство. Все мы знаем, как выглядят обычные домашние или офисные маршрутизаторы. Хотя их размеры уменьшаются с каждой новой моделью, все равно они достаточно большие, и но-

сить с собой такое устройство никто не станет. Мобильные же маршрутизаторы имеют размер со спичечный коробок, поэтому их легко можно носить в кармане, портмоне или женской сумочке. На рис. 3.1 изображен типичный 3G-маршрутизатор. Его размеры: 100×62×16 мм, а вес — 94 грамма. Сильно уменьшить размеры подобного устройства вряд ли получится, поскольку большей частью своих габаритов оно обязано аккумулятору — именно из-за него устройство получило высоту в 10 см. А иначе его можно было бы создать размером с обычную флешку.



Рис. 3.1. 3G-маршрутизатор Wi-Fi TP-Link TL-MR3040

Преимуществ у этого решения несколько:

- ради дешевого Интернета не придется менять ни привычного оператора, ни привычный тариф, ни рассылать друзьям-абонентам свой новый номер. Тем более, что замена номера в наши дни — довольно проблематичное занятие, поскольку к номеру телефона «привязываются» некоторые онлайн-службы, системы электронных платежей, платежные карты и т. п.;

  Освобождение от «мобильного рабства»

  Справедливости ради надо отметить, что в России совсем недавно заработала-таки система освобождения от «мобильного рабства», и абонентам мобильных сетей предоставлена возможность уйти к другому оператору со своим номером.

  На Украине вроде бы тоже имеется такая возможность, но, на мой взгляд, — это совсем не есть так хорошо, как задумывалось. Сейчас хоть понятно, у кого какой оператор. Допустим, мой тарифный план в сети МТС предусматривает 50 минут бесплатных звонков в день. Кто-то оставил свой номер (например, 050) и перешел на Лайф. Я звоню ему, думая, что звонок будет бесплатным, а на самом деле он тарифицируется совсем иначе. Так что сделано все это не для заботы об абоненте, а для получения дополнительной прибыли.

- если в своем автомобиле в качестве навигатора вы используете планшет, он тоже сможет подключиться к тому же мобильному маршрутизатору для получения доступа к Интернету, и вам не придется покупать для планшета отдельную SIM-карту. Аналогично, если вы отправляетесь в путешествие с друзьями или семь-

ей, все находящиеся в машине смогут использовать один маршрутизатор для доступа к Интернету. Однако нужно помнить, что скорость доступа в таком случае снижается пропорционально количеству подключенных устройств;

- мобильный маршрутизатор вы можете использовать и дома для подключения всех нуждающихся в Интернете устройств, и ноутбуков в том числе. Некоторые производители заявляют радиус действия маршрутизатора до 50 метров, на практике выходит до 10 метров, однако этого в большинстве случаев вполне достаточно. К тому же никто не мешает поднести маршрутизатор поближе к ноутбуку. Кстати, большинство мобильных маршрутизаторов могут подключаться к компьютеру по USB, а это значит, что подзарядка аккумулятора маршрутизатора будет от этого USB и осуществляться.

Конечно, есть у этого способа и недостатки. И первый из них — это цена мобильного маршрутизатора. Некоторые операторы предоставляют маршрутизаторы за символическую плату, но, как правило, они потом отыгрываются на тарифах. Поэтому, хоть это и «кусается», но лучше все же купить свой собственный маршрутизатор. А потом вы вольны выбрать себе любого оператора связи.

Второй недостаток — это скорость. Учитывая, что сигналы Wi-Fi имеют привычку «теряться», скорость, даже при условии подключения к маршрутизатору одного клиента, окажется немного ниже заявленной. А вот при подключении нескольких клиентов скорость упадет пропорционально их числу. Например, если на практике для одного устройства вам удается держать скорость 512 Кбит/с, то при подключении второго (пусть вы предоставили пароль для доступа к маршрутизатору своему другу) скорость будет снижена до 256 Кбит/с для каждого устройства.

Третий недостаток — все-таки мобильный маршрутизатор это автономное устройство, и время его работы ограничено емкостью аккумулятора. В среднем мобильные маршрутизаторы могут автономно работать до 4 часов, затем потребуется их подзарядка. Если вы используете такой маршрутизатор в автомобиле, это вообще не проблема — достаточно приобрести автомобильную USB-зарядку. Но вне источника питания (например, в парке, в общественном транспорте) мобильный маршрутизатор сможет продержаться лишь половину рабочего дня. В общем-то, тоже неплохо, учитывая, что вы не постоянно находитесь в Интернете, а во время простоя такие устройства переходят в энергосберегающий режим.

Использовать мобильный маршрутизатор или нет — решать только вам. Однозначно могу сказать, что если вы решитесь им обзавестись, вопрос «куда девается трафик?» перестанет вас волновать, как и стоимость доступа к Интернету (многие безлимитные тарифные планы предусматривают фиксированную плату за каждый день пользования).

3.3. Программные способы снижения расхода трафика

Если аппаратное решение, предложенное в предыдущем разделе, вас не вдохновляет, перейдем сугубо к программным решениям. И сначала разберемся, на что уходит трафик при работе с Android:

- обновления программ через Google Play Маркет;
- обновления различных виджетов;
- обновления самой системы Android;
- потребление трафика установленными программами;
- синхронизация аккаунтов.

Что делать, чтобы уменьшить расход трафика, думаю, уже понятно: отключить автоматическое обновление, виджеты и выбрать менее прожорливые программы. Как правило, бесплатные программы часто содержат рекламу, а в их платных версиях реклама не отображается. Вот и подумайте — может, имеет смысл заплатить 1–2 доллара за платную версию, чем платить каждый месяц на 1–2 доллара больше за Интернет?

Далее мы рассмотрим каждый из пунктов «расходной части» трафика подробно.

3.3.1. Обновления программ через Google Play Маркет

Обновление программ — дело полезное, однако производить его нужно только, когда вы подключены к стационарной сети Wi-Fi, а даже не к сети мобильного маршрутизатора, описанного в *разд. 3.1*. Скорость такого маршрутизатора не очень высока, а время автономной работы ограничено — вы же не хотите, чтобы обновление программы не было завершено? Например, то же приложение Real Racing при его первом запуске загружает на ваше устройство до 1 гигабайта данных. А что, если во время загрузки этого объема данных (довольно внушительного даже для современных мобильных соединений) или его обновления в будущем «сядет батарейка» в вашем маршрутизаторе? С Android, конечно, ничего плохого не произойдет, а вот приложение может потом перестать запускаться.

Поэтому обновлять программы и дешевле, и безопаснее только после подключения к стационарной сети Wi-Fi. Даже если вы не дома, а обновить приложение уж очень хочется, можно найти сеть поблизости — бесплатные точки доступа часто расположены в библиотеках, отелях, кафе, ресторанах, мойках, автосервисах и т. п. Чтобы Android не пыталась обновить приложения самостоятельно и когда ей вздумается, лучше отключите их обновление вовсе. Всегда можно, получив уведомление об обновлении (оно отображается в области уведомлений), обновить приложение вручную, предварительно подключившись к сети Wi-Fi.

Для отключения обновления приложений выполните следующие действия:

- запустите приложение Play Маркет;
- откройте меню приложения (рис. 3.2) и выберите команду **Настройки**;
- для параметра **Автообновление приложений** установите значение **Никогда** (рис. 3.3).

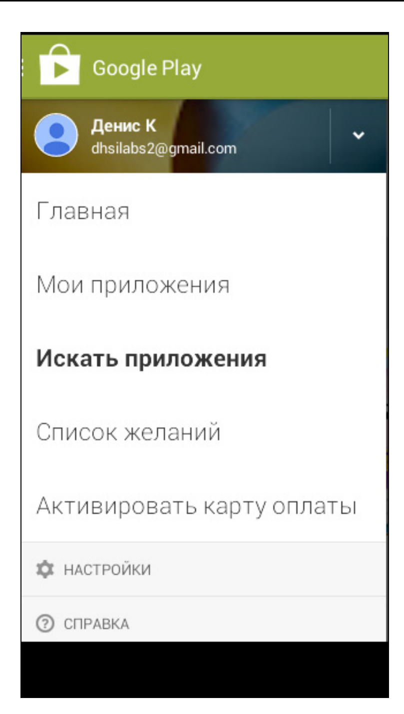


Рис. 3.2. Меню Google Play Маркет

11:09
Настройки
ОБЩИЕ
Уведомления
Сообщать о выходе обновлений для моих игр и приложений
Автообновление приложений
Никогда
Добавлять значок на главный экран
Для новых приложений
Очистить историю поиска
Удалить информацию о всех ваших поисковых запросах
ЛИЧНЫЕ
Настроить фильтр
Чтобы предотвратить загрузку нежелательных приложений, настройте фильтрацию контента

Рис. 3.3. Отключение автоматического обновления приложений

3.3.2. Обновления различных виджетов

Прогноз погоды, новости, курсы валют — все эти виджеты требуют обновления информации из Интернета. Если вы навешали на рабочий стол кучу виджетов, готовьтесь к расходу трафика. Решений два: или отключить виджеты, или смириться. Когда вы находитесь в зоне действия Wi-Fi, обновление виджетов для вас бесплатно, а вот как только вы выходите за ее пределы, информация будет передаваться по 3G-соединению, а за это оператором взимается плата.

3.3.3. Обновления самой системы Android

Обновление самой Android также потребляет трафик. Здесь лучше всего перейти в меню **Настройки | О телефоне | Обновление системного ПО** (или **Настройки | О планшетном ПК | Обновление системы** — в зависимости от используемой версии Android и типа устройства) и выбрать опцию **Спрашивать перед загрузкой**. В результате, когда будет доступно обновление, система спросит вас, нужно ли его загружать. Если вы подключены к Интернету по Wi-Fi, можно загрузить обновление или же отложить загрузку, чтобы не тратить дорогой 3G-трафик.

3.3.4. Трафик установленных программ

Некоторые приложения, особенно интернет-приложения, потребляют определенный трафик, и это нормально. Такими приложениями являются, например, Skype, uTorrent и другие подобные программы. Даже если смартфон заблокирован, то это не означает, что эти приложения не работают. Skype, когда им не пользуются, потребляет совсем немного трафика, но потребляет. А вот uTorrent может вызвать значительный перерасход трафика. Допустим, вы находились дома, подключение осуществлялось по Wi-Fi, и вы скачали на ваш смартфон с торрентов музыку или фильмы. Когда же вы вышли из дому (за пределы сети Wi-Fi), uTorrent продолжил раздачу загруженного контента другим пользователям, но при этом подключение к Интернету осуществлялось уже через сеть вашего мобильного оператора. То есть, теперь за трафик вы платите свои кровные.

Как решить эту проблему? Главное — не забыть перед выходом на улицу закрыть все приложения, которые потенциально могут получать доступ к Интернету. Просмотреть список запущенных приложений можно через меню **Настройки | Приложения | Работающие** (рис. 3.4). Здесь видно, что в данный момент кроме всех прочих приложений запущено приложение Skype, которое может быть причиной утечки трафика.

Другое дело, когда вы не знаете точно, какая именно программа обращается к Интернету и расходует трафик. Помочь в этом могут программы-брандмауэры. Они отслеживают, что за программы получают доступ к сетевым ресурсам, и при необходимости блокируют их. Если трафик расходует какая-то вредоносная программа или та, которая не должна вообще расходовать трафик — например, какой-то несетевой пасьянс, но ее нечестные разработчики что-то отправляют с вашего устройства, то вы можете ее заблокировать, а потом, разобравшись, как она попала к вам

на устройство, — удалить. В общем, следует понять, какие программы получают доступ к Интернету, а потом уже вы сами разберетесь, что с ними делать — или блокировать их, или удалять.

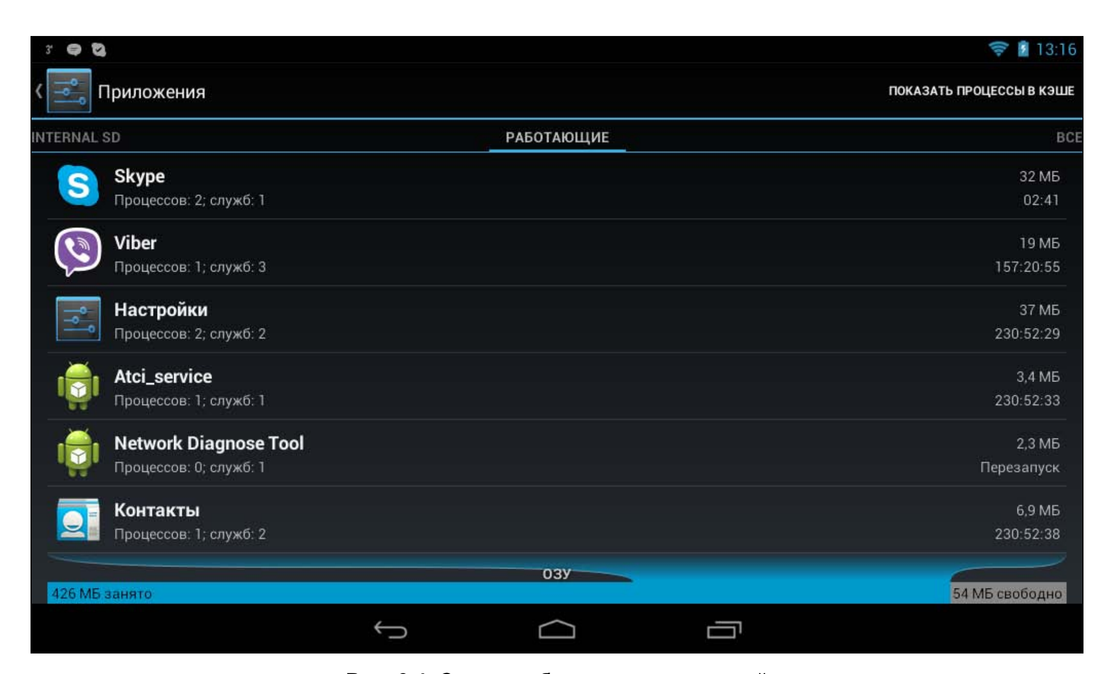


Рис. 3.4. Список работающих приложений

В настоящее время популярны следующие брандмауэры для Android: Android Firewall, DroidWall, avast! Mobile Security для Android, NoRoot Firewall. Программа Android Firewall устанавливается на современные версии Android (4.*x*), а программу DroidWall можно использовать на ее устаревших версиях (1.6, 2.*x*). Обе эти программы работают сугубо как брандмауэры, не делая ничего больше, а вот программа avast! Mobile Security является и брандмауэром, и антивирусом.

Недостаток всех трех упомянутых программ — они требуют для своей работы root-доступа, а получение такого доступа, как я уже неоднократно предупреждал, чревато двумя проблемами. Во-первых, даже если все пройдет успешно, ваше устройство автоматически теряет гарантию производителя. Во-вторых, если что-то пойдет не так, вы превратите свой смартфон в «кирпич», не реагирующий ни на что. В сервис-центре вам если и помогут, то за ваш счет.

На свой страх и риск

В *главе 10* мы рассмотрим, как получить root-доступ, однако если что-то пойдет не так, то ни автор книги, ни издательство не несут ответственности за ваши действия. Вы будете действовать на свой страх и риск.

Преимущества root-доступа тоже сомнительны. Да, вы сможете установить брандмауэры, антивирусы и другие приложения, тесно интегрирующиеся с системой и позволяющие защитить ее от разных угроз. С другой стороны, пока у вас нет root-

доступа, большинство угроз вам и не страшны, поскольку вредоносный код ничего не сможет сделать с Android, если запущен от имени пользователя, у которого нет root-доступа. Выводы делайте сами.

Последним в нашем списке упомянут брандмауэр NoRoot Firewall (Брандмауэр без Root). Вот это то, что нам нужно. Самое главное, что для работы брандмауэра NoRoot Firewall не нужны права root, а это означает, что вы не испортите свое устройство его установкой. Брандмауэр NoRoot Firewall дает возможность создавать простые фильтры, позволяющие блокировать доступ некоторых приложений к Интернету, а также умеет блокировать интернет-ресурсы по имени и IP-адресу. Вряд ли вы станете сами устанавливать какие-то правила, поэтому сейчас мы рассмотрим, как выполнить то, что необходимо большинству пользователей, а именно — определить, каким программам нужен доступ к Интернету и разрешить/запретить этот доступ.

Прежде всего нужно установить программу. На рис. 3.5 показано, как выглядит страница ее установки в Play Маркет, — чтобы вы ничего не перепутали и установили именно то приложение.

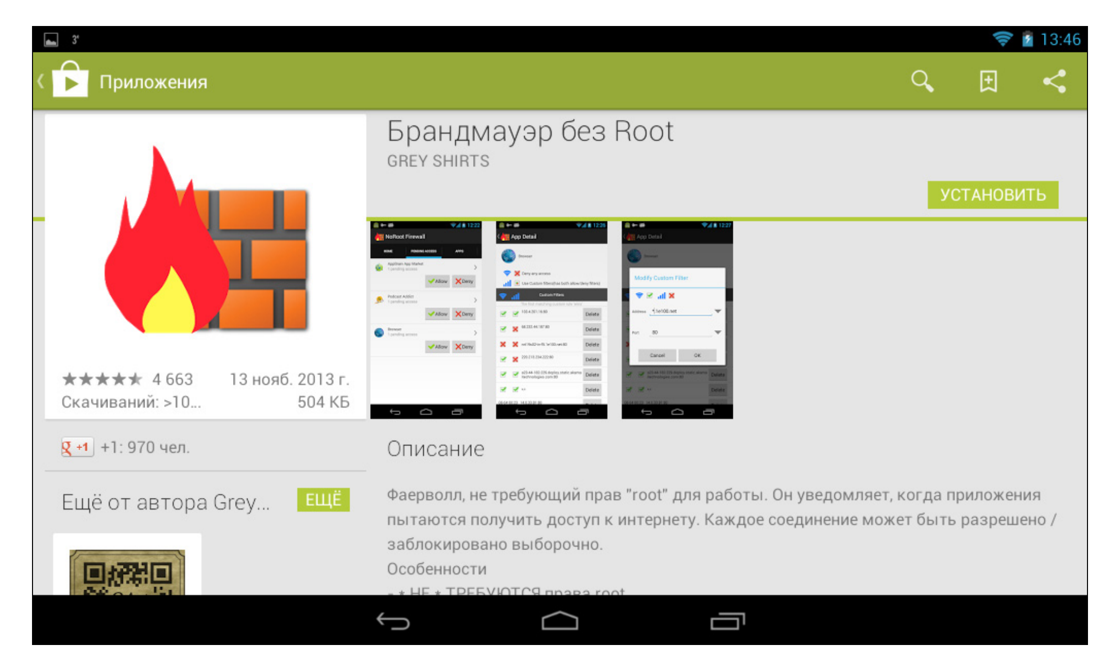


Рис. 3.5. Установка брандмауэра

Запустите установленное приложение. На вкладке **Домой** нажмите кнопку **Запустить** (рис. 3.6) для запуска VPN-соединения.

Поскольку приложение не требует root-прав, оно работает посредством создания VPN-соединения, через которое будет проходить весь ваш трафик, что и позволит приложению его контролировать. Собственно, об этом и предупредит вас Android (рис. 3.7).

Рис. 3.6. Нажмите кнопку **Запустить**

Рис. 3.7. Предупреждение о перехвате трафика

После запуска VPN-соединения доступ к Интернету всем приложениям будет автоматически заблокирован. На вкладке **Ожидающие доступа** (рис. 3.8) вы увидите перечень всех приложений, которые пытаются в данный момент «достучаться» до Интернета. В моем случае это сама Android и ее службы Google, Skype и Viber. Чтобы разрешить приложению доступ к Интернету, нажмите соответствующую ему кнопку **Разрешить**.

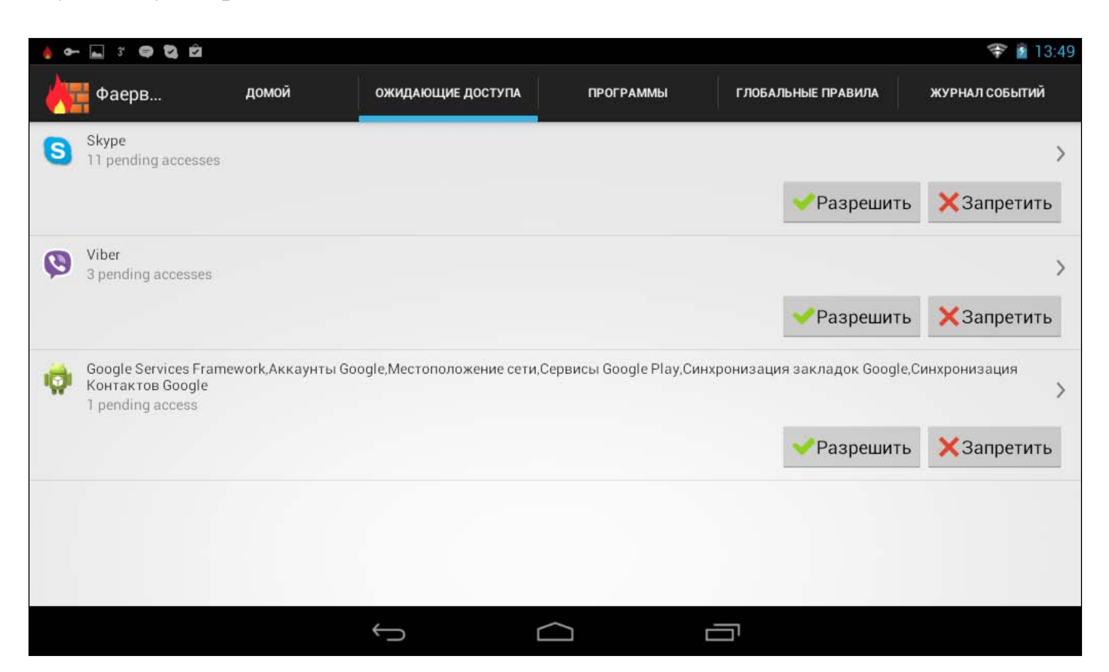


Рис. 3.8. Приложения, пытающиеся получить доступ к Интернету

Как видите, в использовании программы нет ничего сложного, и она позволяет быстро определить, какие приложения пытаются получить доступ к Сети.

А что делать, если у вас нет времени изучать, какая программа вызывает перерасход трафика, на счету остался последний рубль, и вы хотели бы его сохранить и не позволить приложениям потратить и его? Для этого есть весьма радикальное решение — программа APN OnOff, позволяющая вывести на рабочий стол плагин, который полностью отключает мобильный Интернет. Теперь вам осталось просто нажать соответствующую кнопку, и мобильный Интернет будет выключен без необходимости путешествия по дебрям меню. Установить эту программу можно по ссылке:

https://play.google.com/store/apps/details?id=com.curvefish.widgets.apnonoff

На устройствах Samsung (поскольку на них используется немного видоизмененный интерфейс Android — TouchWiz) в области уведомлений имеется кнопка **Мобильные данные**, которая включает/выключает передачу данных по 3G-сети (рис. 3.9). Поэтому на таких устройствах нет необходимости в каких-либо сторонних программах или плагинах для отключения/включения передачи мобильных данных.

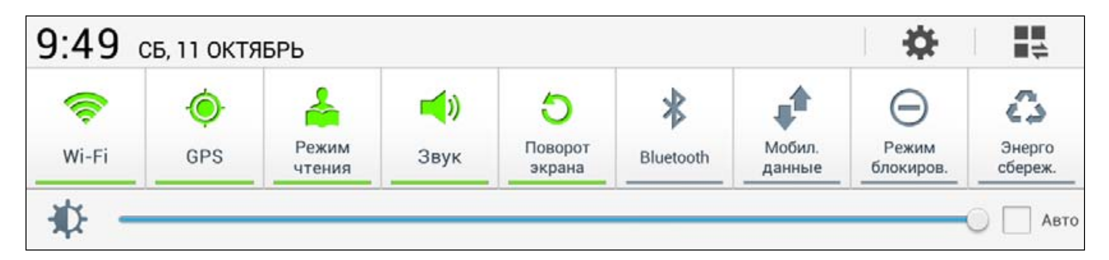


Рис. 3.9. Кнопка **Мобильные данные**

3.3.5. Синхронизация аккаунтов

Прежде чем перейти к следующей главе, рассмотрим еще одну причину расхода трафика — синхронизацию аккаунтов. При первом включении устройства пользо-

Рис. 3.10. Настройка синхронизации

вателю предоставляется выбор: или использовать существующий аккаунт Google, или создать новый. Настроив синхронизацию аккаунтов на всех своих устройствах (стационарном компьютере, ноутбуке, планшете, мобильном телефоне), вы сделаете работу гораздо удобнее. Например, если вы внесли контакт в адресную книгу смартфона, он же появится и на вашем планшете. Если вы на ноутбуке посетили какой-то сайт, благодаря синхронизации вы сможете получить к нему доступ и на планшете, и на смартфоне, просмотрев историю посещений. Все это очень удобно, но синхронизация может потреблять лишний трафик, особенно если задана синхронизация фотографий, электронной почты и т. п.

Настроить синхронизацию очень просто — выберите меню **Настройки**, далее в области **Аккаунты** опцию **Google**, затем ваш аккаунт, а потом определите, что нужно синхронизировать, а что — нет (рис. 3.10). Из рис. 3.10 видно, что я выключил синхронизацию **Медиа** и **Google Фото**. Все остальное синхронизируется. Если же нужно вовсе отключить синхронизацию, снимите все флажки.

3.4. Приложение Wi-Fi Analyzer

Найти ближайшую сеть Wi-Fi (а значит, сэкономить 3G-трафик и ваши деньги) поможет программа Wi-Fi Analyzer. Программа абсолютно бесплатная и установить ее можно из Play Маркет.

В меню **Вид** выберите режим **Список AP** — вы получите список точек доступа (рис. 3.11) с разной полезной информацией о них. По уровню сигнала можно судить, как близко вы находитесь к той или иной сети Wi-Fi. На рис. 3.11 видно, что

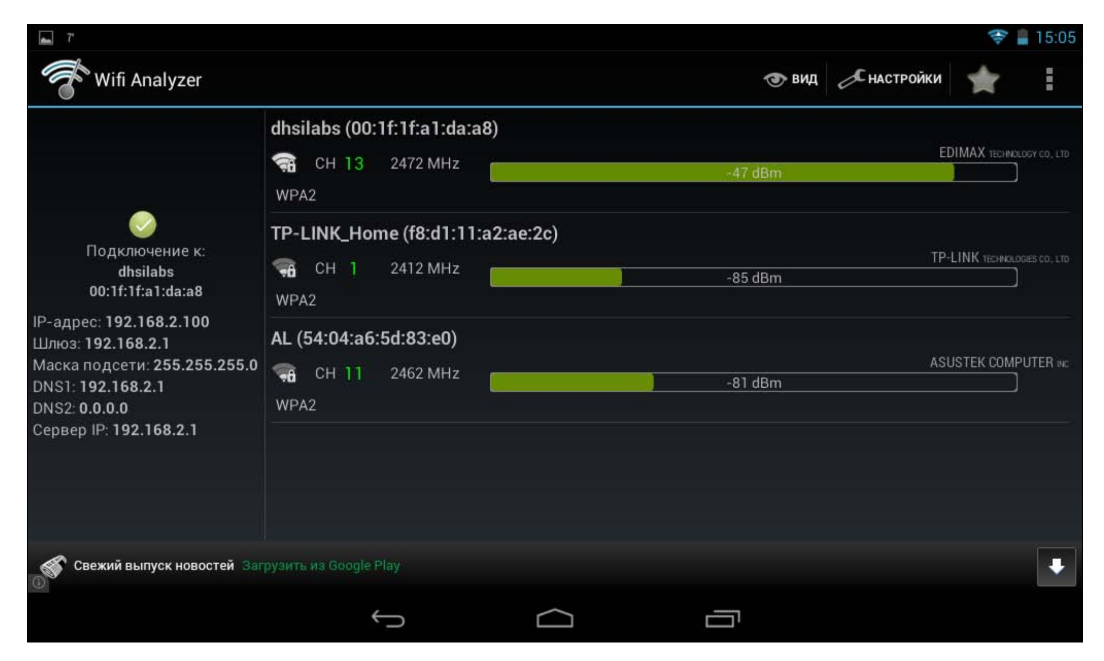


Рис. 3.11. Список точек доступа

устройство подключено к сети **dhsilabs**, и что эта сеть находится ближе всего к устройству. Показано также, что все три доступные сети являются закрытыми (частными), о чем свидетельствует замок в нижнем правом углу значка Wi-Fi. Подключиться к этим сетям без знания пароля, увы, не получится.

Тем не менее, это приложение поможет выбрать ближайшую открытую сеть с лучшим сигналом. Иногда в торговых центрах устанавливается несколько точек доступа, и, используя Wi-Fi Analyzer, можно выбрать лучшую сеть.

Как уже было отмечено, значок сети уведомляет пользователя об уровне сигнала и о том, закрыта ли сеть паролем. Но Wi-Fi Analyzer помимо значка выводит также и тип аутентификации — например: WPA2 — самый надежный, WPA — чуть хуже, а WEP — вообще решето. Но я вам об этом ничего не говорил...

Кроме того, в режиме **График каналов** (рис. 3.12) показывается наложение (интерференция) каналов соседних сетей. Представим, что есть три сети А, Б и В. Сети А и В спроектированы так, что они находятся или на одном и том же канале, или на соседних каналах (например, 1 и 3). Из-за этого возникает интерференция сигналов, и скорость передачи данных по таким сетям оставляет желать лучшего. Тогда лучше выбрать сеть Б, которая удалена от сетей А и В. На рис. 3.12 показано, что интерференция сигналов возникает между сетями **AL** и **dhsilabs**.

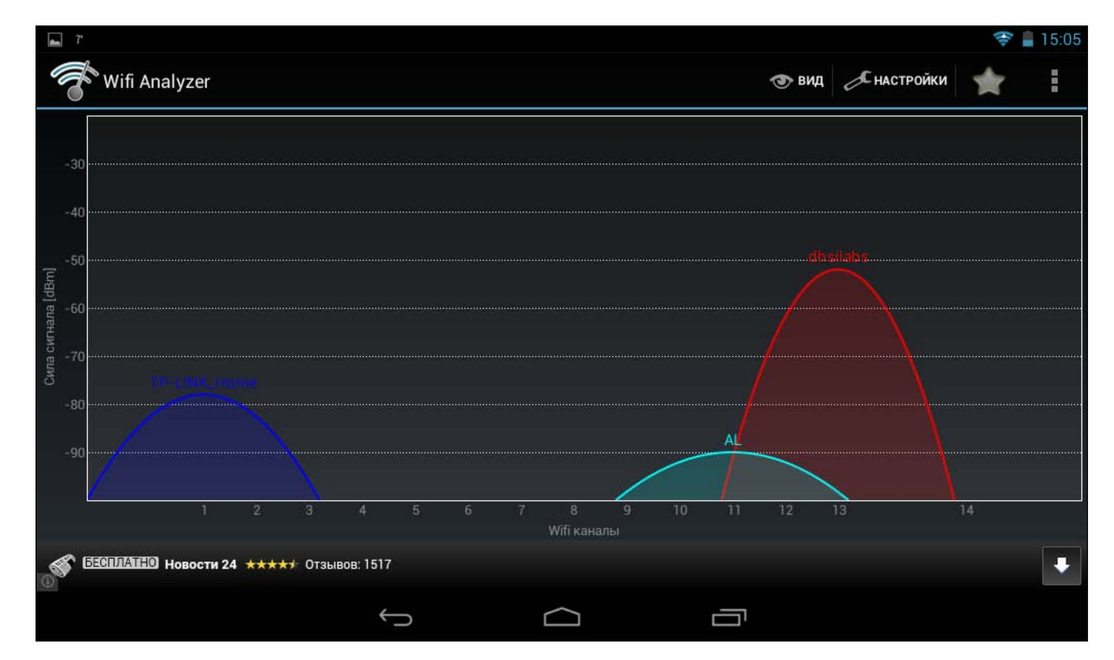


Рис. 3.12. График каналов

Программу Wi-Fi Analyzer можно использовать не только для поиска бесплатных сетей с лучшим сигналом, но и для тонкой настройки своей домашней сети. Допустим, вы определили, что соседние беспроводные сети работают на каналах 1, 3, 6 и 7. Тогда для своей сети выберите канал, который бы отличался как минимум на 3 канала от соседней сети. В нашем случае можно использовать каналы 10, 11, 12 и

13 — чем дальше, тем лучше. Поэтому, если другие сети больше не появятся, можно смело занимать канал 13 как самый удаленный.

3.5. Сжатие трафика в популярных браузерах

Еще один способ сэкономить трафик — использовать программы для его сжатия. А вот как сжимать и чем сжимать, сейчас мы и разберемся.

Для начала нужно понять, как работает сжатие трафика. Представим, что у нас есть браузер с функцией сжатия трафика. Вы хотите посетить сайт автора этой книги **http://dkws.org.ua**. При выключенном сжатии браузер сразу обращается к серверу **dkws.org.ua**, получает страницу и отображает ее вам. При включенном сжатии браузер обращается к собственному серверу с просьбой получить сайт **http://dkws.org.ua**. Тогда удаленный сервер получает запрашиваемую страницу, сжимает ее и отправляет нашему браузеру. Наш браузер, получив сжатую страницу, распаковывает ее и отображает.

Как видите, все предельно просто. Однако нужно учитывать, что запрошенные вами страницы будут открываться немного медленнее. Все зависит от «веса» самой страницы. Ведь распаковка данных нагружает процессор устройства, из-за чего, особенно, если на устройстве запущено много других приложений, может наблюдаться снижение его производительности. С другой стороны, если страница большая, а ваше мобильное соединение медленное, особой разницы вы не почувствуете даже несмотря на то, что страница передается в сжатом виде, и вместо, скажем, 7 Мбайт вам нужно получить всего 2 Мбайт. Понятно также, что не все страницы хорошо сжимаются. Если на странице много текста, она сжимается очень сильно. Если же вы открываете страницу, где много фотографий, сжатие уже не будет столь эффективным, поскольку фотографии, как правило, распространяются в формате JPEG, который уже является сжатым. Можно, конечно, еще больше ужать JPEG за счет снижения качества изображения, но о существенной экономии трафика мечтать вряд ли приходится. Однако в любом случае снижение трафика все равно будет, так что на мобильных устройствах функция сжатия трафика как никогда актуальна.

Изначально функция сжатия присутствовала в браузере Opera. С этой функцией я, как и многие другие пользователи, познакомился еще на настольных системах. Opera тогда был единственным браузером, предоставляющим подобную функцию. Позже, когда у меня появилось Android-устройство и вместе с ним необходимость экономии мобильного трафика, я установил Android-версию Opera. Хорошо, что функция сжатия трафика была портирована в Android-версию, где она более востребована, чем на настольных системах.

Для включения сжатия нажмите на логотип Opera — появится меню, в котором, помимо всего прочего, можно будет включить сжатие, установив переключатель в положение **ВКЛ** (рис. 3.13).

После включения сжатия в этом меню (под переключателем) станет выводиться информация о степени сжатия. В данном случае экономия трафика составила 74 %,

поскольку из 7,6 Мбайт объема страницы было получено всего 2 Мбайт сжатого трафика.

Позже функция сжатия появилась и в браузере Google Chrome. Для ее активации откройте меню браузера, выберите пункт **Настройки**, перейдите в раздел **Пропускная способность**, выберите **Сокращение трафика** и установите переключатель в положение **Включено** (соответственно, для выключения сжатия нужно установить переключатель в положение **Выключено**).

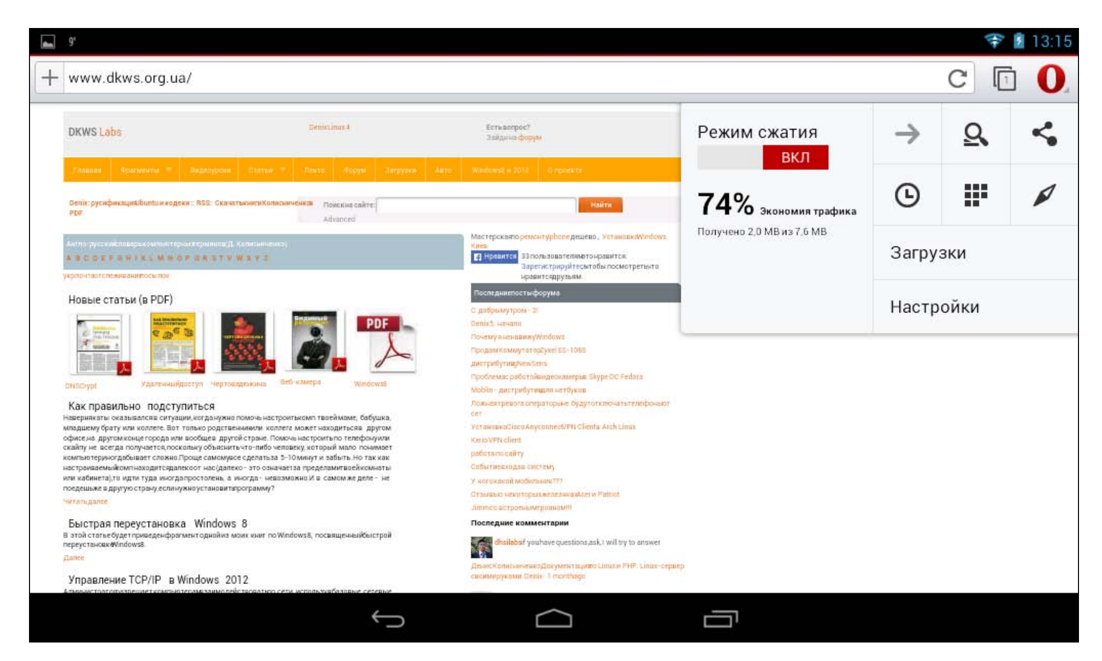


Рис. 3.13. Включение сжатия в Opera

В браузере Google Chrome есть еще одна полезная опция, правда, она не экономит трафик, а, наоборот, его расходует. Функция называется **Предварительная загрузка веб-страниц**. Представим, что вы открыли страницу, на которой есть ссылки А, Б и В. Если включена предварительная загрузка страниц, тогда страницы, на которые указывают ссылки А, Б и В, будут загружены предварительно, еще до того момента, как вы на них перейдете.

С одной стороны, функция полезная, поскольку переход на страницы по ссылкам А, Б и В осуществляется моментально. Пока вы читаете основную страницу, дополнительные уже загружены браузером. При переходе по ссылке браузеру их загружать не придется, надо будет только их отобразить. Поэтому всем кажется, что браузер Chrome работает гораздо быстрее других. С другой стороны, расход трафика при этом колоссальный. Вы ведь можете перейти только по ссылке А или вообще ввести другой адрес сайта — получается, что все предварительно загруженные страницы были загружены зря.

Поэтому функцию предварительной загрузки нужно или отключить, или хотя бы убедиться, что предварительная загрузка страниц осуществляется только через

Wi-Fi (рис. 3.14). Добраться до этой функции можно через меню **Настройки | Пропускная способность | Предварительная загрузка веб-страниц**.

На своих устройствах я для оптимизации работы держу функцию сжатия включенной в браузере Opera (который использую при работе через 3G), а браузер Chrome запускаю только при работе через Wi-Fi.

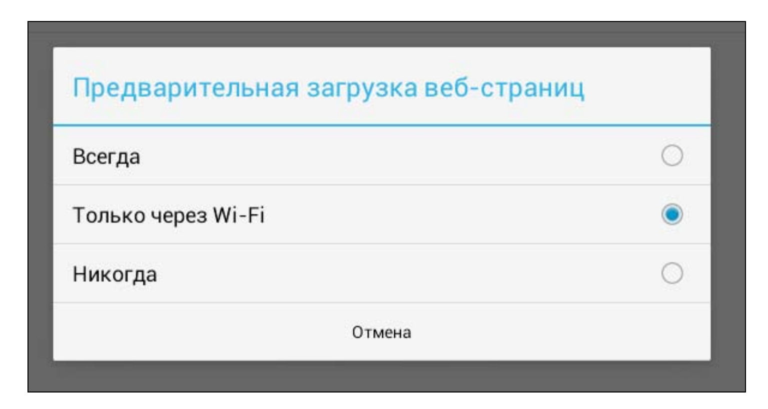


Рис. 3.14. Предварительная загрузка страниц

Если вы боитесь, что можете забыть и по привычке запустить браузер без активной функции сжатия, установите приложение Browser Toggle, позволяющее выбрать, какой браузер использовать для мобильного соединения, а какой — для Wi-Fi. Установить это приложение можно по ссылке:

https://play.google.com/store/apps/details?id=com.gombosdev.browsertoggle

Запустите приложение (рис. 3.15) — первая кнопка позволяет выбрать браузер для мобильного соединения (рис. 3.16), вторая кнопка — для соединения Wi-Fi (рис. 3.17).

Для мобильного соединения установите браузер, где вы включили функцию сжатия, а для соединения Wi-Fi — тот браузер, где функция сжатия выключена.

На рис. 3.18 видно, что для мобильного соединения я установил браузер Chrome, а для Wi-Fi — Opera (обычно я использую эти браузеры наоборот, но сейчас хотелось поэкспериментировать с программой).

Конечно, если вам и этого мало (ну или трафика осталось совсем мало), можно воспользоваться полностью текстовым браузером TextOnly Browser. Этот браузер отображает текст и ничего кроме текста. Лично мне использовать этот браузер не очень удобно, но когда предоплаченного трафика осталось 1–2 Мбайт, то и этому браузеру будешь рад. Установить TextOnly Browser можно по ссылке:

https://play.google.com/store/apps/details?id=com.spacenext.textonly

Запустите браузер и перейдите в меню **Настройки | Передача данных**. Здесь вы увидите графики расхода трафика и приложения, которые его расходуют. Если браузер у вас — основной потребитель трафика, то цель достигнута, и дальше можно ничего более не делать. Но, например, у меня основным потребителем трафика является Skype (рис. 3.19).

8:50

BrT Settings

Select browser for mobile connections:

Please, select a browser!

Select browser for WiFi connections:

Please, select a browser!

Clear default system browser:

Clear

Select and set default system browser (Unfortunately this action will start the browser with "http://google.com" immediately. Please just close the browser!):

Select

Рис. 3.15. Интерфейс программы

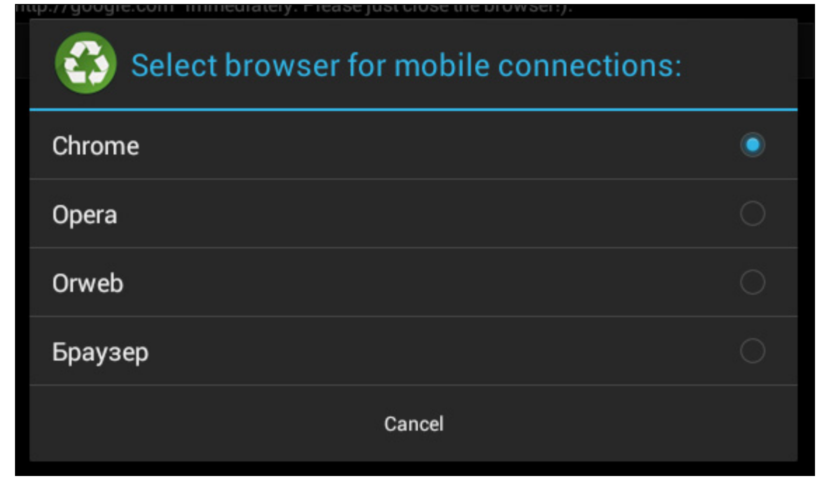


Рис. 3.16. Выбор браузера для мобильного соединения

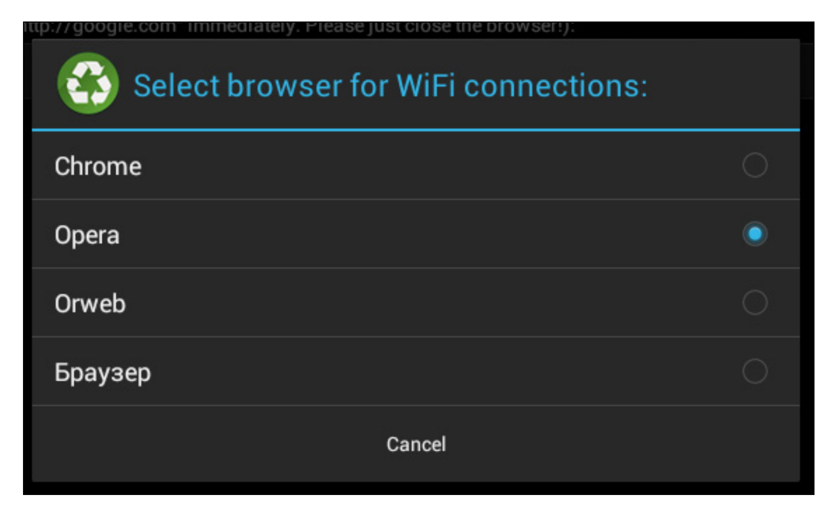


Рис. 3.17. Выбор браузера для Wi-Fi

8:51
BrT Settings
Select browser for mobile connections:
Chrome
Select browser for WiFi connections:
Opera
Clear default system browser:
Clear
Select and set default system browser (Unfortunately this action will start the browser with "http://google.com" immediately. Please just close the browser!):
Select

Рис. 3.18. Браузеры выбраны

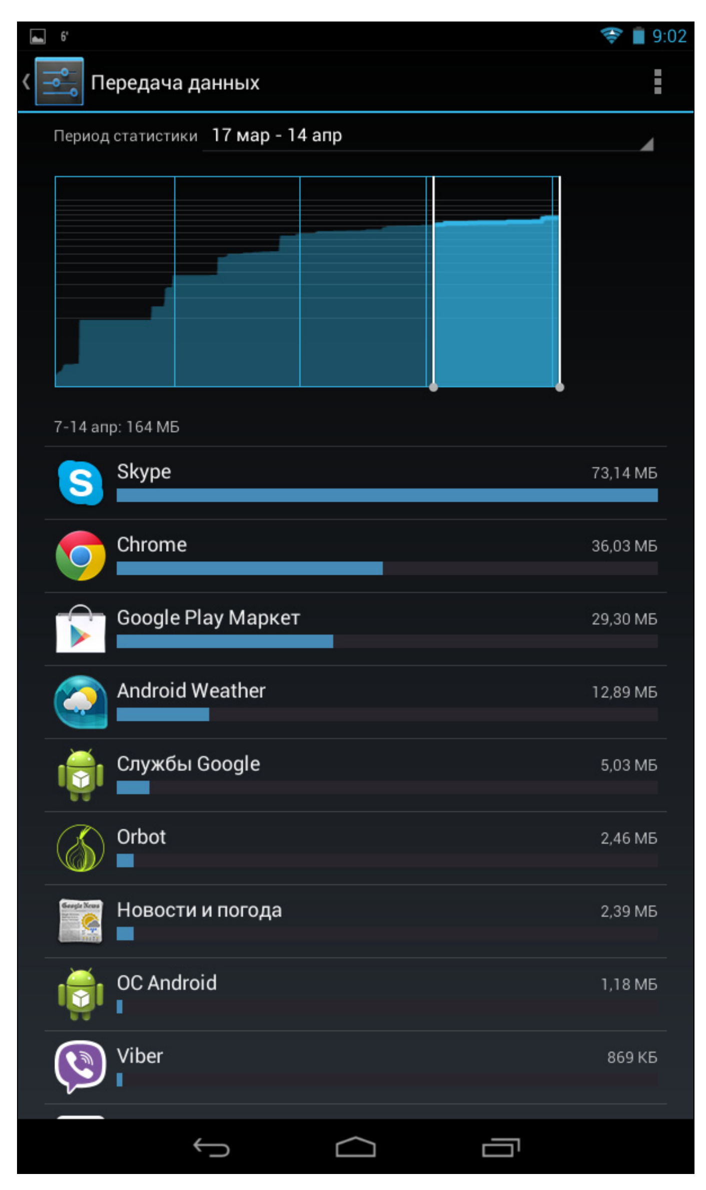


Рис. 3.19. Отчет о потреблении трафика

И в случае, когда основным потребителем трафика является сторонняя программа, тогда нужно использовать программы, которые сжимают весь трафик, а не только трафик браузера.

Хорошо себя зарекомендовала в этом плане программа **Onavo Extend | Data Savings**. Она эффективно сжимает весь входящий трафик (исходящий трафик не сжимается, это понятно, ведь удаленная сторона не знает, что он сжатый и не сможет его распаковать). Установить это приложение можно по ссылке:

https://play.google.com/store/apps/details?id=com.onavo.android.onavoics

У программы **Onavo Extend | Data Savings** есть одна особенность — она работает только на Android версии 4.*x*, и на более старых версиях работать не будет.

1. Итак, установите и запустите **Onavo Extend | Data Savings**.
2. Нажмите кнопку **Continue**, а затем кнопку **Agree & Continue** (этим вы принимаете лицензионное соглашение).
3. Программа попытается создать VPN-подключение. Установите флажок **Я доверяю этому приложению** и нажмите кнопку **OK** (рис. 3.20).

После этого программа начнет работать. Вы можете запускать любые сетевые приложения, и весь их трафик будет проходить через созданное VPN-соединение. Исходящий трафик станет отправляться без сжатия — как есть, а вот входящий будет сжиматься. Учтите, что программа контролирует весь ваш трафик и кроме сжатия она может сделать с ним все, что угодно. Следовательно, такое решение явно не для параноиков, которые боятся, что их трафик перехватят.

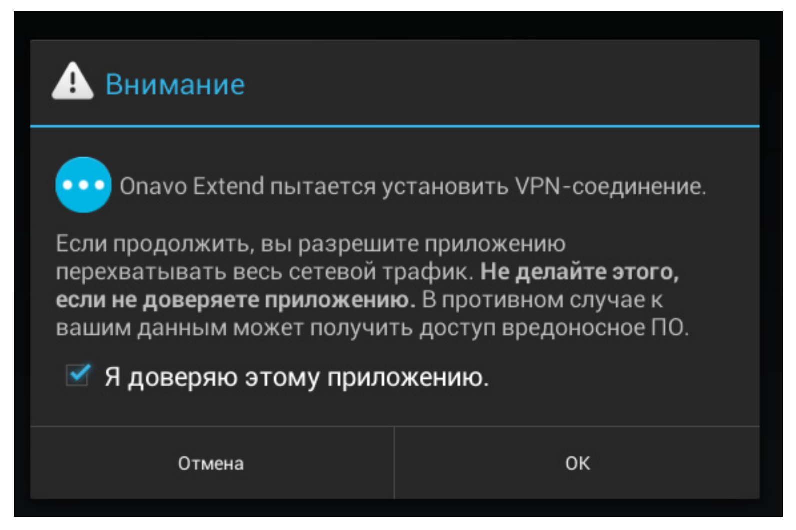


Рис. 3.20. Создание VPN-подключения

Нужно отметить, что программа не сжимает трафик, когда вы работаете по Wi-Fi, а также отображает наглядные отчеты об использовании трафика (рис. 3.21).

Казалось бы, мы уже рассмотрели все, что можно: и текстовый браузер, и сжатие трафика в браузере, и программу для сжатия всего трафика. Однако, есть и еще нерассмотренные возможности.

Так, если вы часто работаете с электронной почтой — например, отправляете документы по e-mail, используйте архиваторы. В Play Маркет представлено множество программ-архиваторов:

- ZArchiver;
- AndroZip File Manager;
- RAR для Android;

- 7Zipper;
- LHAndroid.

Все программы я перечислять не стану — поверьте, в Play Маркет можно найти программу-архиватор на любой вкус.

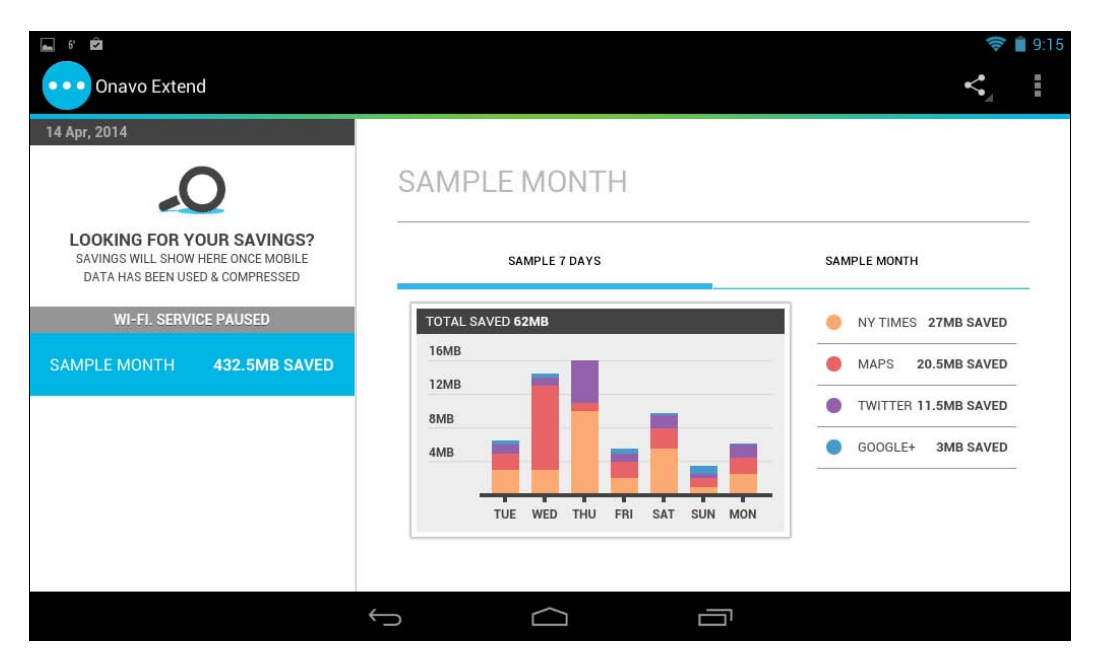


Рис. 3.21. Программа не работает по Wi-Fi и отображает наглядные отчеты

Сжимайте все отправляемые файлы. Хорошо сжимаются офисные документы, картинки в некоторых несжатых форматах (BMP, TIFF и др.), текстовые файлы.

Надеюсь, с помощью советов из этой главы вы победили перерасход трафика, а в следующей главе мы поговорим о том, как защитить в Android ваши персональные данные.



ГЛАВА 4

Защита персональных данных

4.1. Необходимость и способы защиты данных в устройствах на Android

Современный мобильный телефон уже давно представляет собой небольшой персональный компьютер, но самое главное в нем даже не возможность запуска различных приложений, а то, что он хранит персональные данные пользователя: приватные фотографии, важные документы, номера кредитных карточек и прочую финансовую информацию. О том, как защитить эти данные, мы здесь и поговорим.

Для защиты персональных данных есть несколько возможных подходов — например, запрет запуска определенных приложений, сокрытие файлов и папок с данными, а также шифрование как отдельных файлов, так и всего устройства. Можно использовать любой из этих путей или даже все вместе.

Но прежде всего следует разобраться, от кого или от чего мы будем защищать свои данные. Все угрозы можно разделить на две большие группы: внешние и внутренние. К *внешним угрозам* относятся различные недоброжелательные сайты и вредоносные программы, которые могут ваши персональные данные передать третьей стороне, изменить их или уничтожить. С такими угрозами как-никак, но справляются антивирусы, которые мы рассмотрим в *главе 5*. К внешним угрозам можно отнести и возможность перехвата данных по сети, особенно когда подключение осуществляется через публичную сеть Wi-Fi аэропорта, отеля, библиотеки, кафе и т. п., которую вы не контролируете. Ваши пароли и финансовая информация (хотя она часто шифруется, но все же...) могут «уплыть» третьей стороне. Перехват таких данных на отрезке телефон–оператор маловероятен (разве что их может перехватить сам оператор), и большинство случаев краж передаваемой информации происходит на отрезке телефон–Wi-Fi. Помочь здесь может организация VPN-соединения и туннелирования. Кстати, перехват трафика оператором тогда вам тоже не будет страшен. О том, как это реализовать, мы поговорим в *главе 6*.

А сейчас мы сосредоточимся исключительно на внутренних угрозах. Представим, что ваш телефон попал в руки злоумышленнику. Как именно это произошло — не суть важно. Пусть вы забыли его в офисе, а ваши коллеги шутки ради или из дру-

гих побуждений могли просмотреть ваши фотографии или прочитать документы. Телефон можно потерять, его могут украсть и т. п.

Представим, что некто держит в руках ваш телефон. Первое, что встает на защиту ваших данных — это графический пароль. Если он у вас отключен, самое время его включить. Дополнительная защита никогда не помешает. Если пароль отключен, злоумышленнику достаточно провести пальцем по экрану в указанном направлении, и блокировка будет снята.

Однако графический пароль не панацея. Если у злоумышленника есть чуть больше времени или определенные навыки (см. об этом в *главе 10*), такой пароль можно обойти. Кроме того, ничто не мешает извлечь из телефона карту памяти и прочитать ее на компьютере или на своем телефоне. Чтобы извлечь карту памяти, никакого пароля не нужно. А вот если данные на карте памяти зашифрованы, прочитать их уже не получится. Шифрование — самый надежный способ защиты личных данных.

Если же шифровать данные по каким бы то ни было соображениям вы не хотите, есть и другие способы защиты — например, запрет запуска определенных приложений и сокрытие папок из галереи. Этими способами защиты пренебрегать не рекомендуется. Вот элементарная ситуация — на планшете, как правило, установлен какой-нибудь файловый менеджер, например, весьма популярный ES Проводник. Ваш ребенок взял планшет, чтобы поиграть в любимую игрушку, и случайно запустил файловый менеджер. Что он может наделать дальше — предсказать сложно. Играючи можно удалить все важные файлы безо всякого злого умысла. Другая ситуация — коллега попросил у вас телефон, чтобы просто позвонить. На время звонка он отошел, чтобы никто не слышал, о чем он говорит. Нужно же защитить от просмотра папки и файлы (например, некоторые документы или фотографии), которые не должны видеть посторонние! Ведь тому, в чьих руках оказался ваш телефон, ничего не помешает покопаться в его содержимом. И даже если в хранящихся на телефоне фотографиях нет ничего конфиденциального, согласитесь, неприятно, когда кто-то без вашего ведома их разглядывает. Итак, далее мы рассмотрим основные способы защиты от внутренних угроз.

4.2. Приложение App Lock (Smart App Protector)

Приложение App Lock (Smart App Protector) — это защитник ваших личных данных на любом устройстве под управлением ОС Android. С его помощью можно защитить все: SMS, электронную почту, фотографии, контакты, а также запретить запуск отдельных приложений.

Использовать приложение предельно просто — нужно задать графический ключ, указать, что нужно защищать, и перевести приложение в режим защиты. После этого никто к вашим личным данным доступа не получит. А в платной версии программы предусмотрена возможность организовать фото- и видеосъемку нарушителя, что как раз и поможет обнаружить недобросовестного человека, который попросил ваш телефон якобы позвонить, а сам попытался залезть в хранящиеся на нем личные данные.

Обойти защиту приложения невозможно, если, конечно, быстренько не получить на чужом телефоне права root. А поскольку это дело не пяти минут, вы можете быть уверены, что никто, взявши ваш телефон якобы позвонить (или когда вы оставите его на столе, отойдя из кабинета ненадолго), не сможет добраться до ваших личных данных.

Приложение App Lock имеет одну важную особенность. Если его удалить какими-либо специальными утилитами, то оно унесет вместе с собой все, что защищало. То есть, если некто попытается удалить с вашего телефона это приложение, чтобы получить доступ к защищаемым им данным, то эти данные тоже будут удалены. Во всяком случае это лучше, чем если бы они попали в руки «захватчика». А вы ни в коем случае не должны забыть открывающий приложение графический ключ! Иначе придется очень постараться, чтобы избавиться от приложения без потери данных. И еще — полагаю, не стоит говорить, что для разблокировки экрана и приложения App Lock следует использовать разные графические ключи.

Устанавливая приложение на смартфон, убедитесь, что вы устанавливаете именно App Lock, а не приложение Защита App, которое также есть в Play Маркет. На рис. 4.1 показана страница Play Маркет для приложения App Lock.

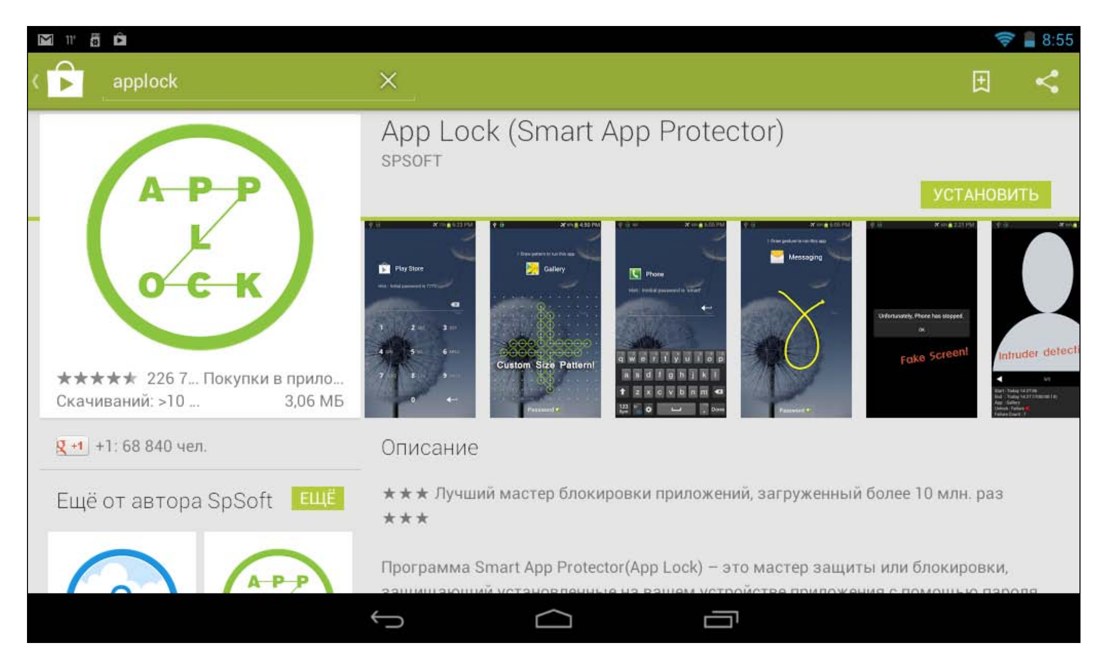


Рис. 4.1. Страница установки приложения App Lock

Установив приложение, запустите его. Оно запросит пароль — введите пароль по умолчанию: `7777`. Рассмотрим основной экран приложения (рис. 4.2). В верхнем правом его углу имеются три кнопки: кнопка защиты (красная — защита выключена, зеленая — включена), кнопка установки пароля и кнопка настроек. Чуть ниже находятся три вкладки:

- **App Lock** — при добавлении приложений на эту вкладку последующее их открытие будет сопровождаться запросом пароля;
- **Screen** — у добавленнных на эту вкладку приложений после их запуска экран будет оставаться постоянно включенным (перестанет выключаться после какого-то времени неиспользования);
- **Rotation** — у добавленных на эту вкладку приложений после их запуска экран не будет изменять ориентации вне зависимости от положения устройства.

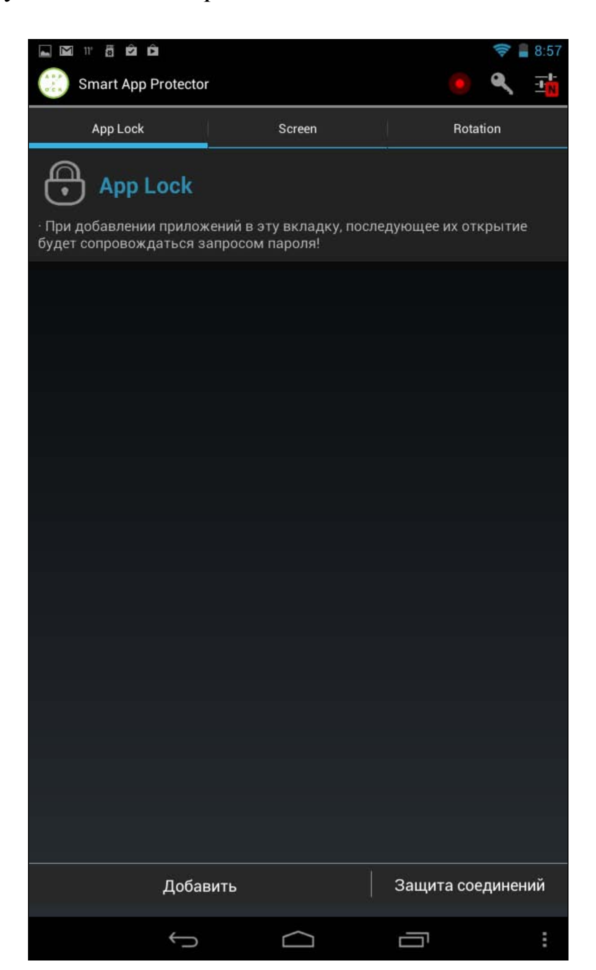


Рис. 4.2. Основной экран приложения App Lock

Для добавления приложений на ту или иную вкладку сначала выберите вкладку, а затем нажмите кнопку **Добавить** внизу окна (рис. 4.3).

На вкладку **App Lock** рекомендуется добавить подлежащие защите приложения. Как правило, это приложения, которые могут содержать конфиденциальные данные (GMail, Skype, Viber, Галерея, Google Talk, Google+, My WebMoney и т. п.), а также те, использование которых может быть потенциально опасным (ES Проводник, Total Commander, Настройки и т. п.). На рис. 4.4 приведен список приложений, которые я защитил на своем планшете.

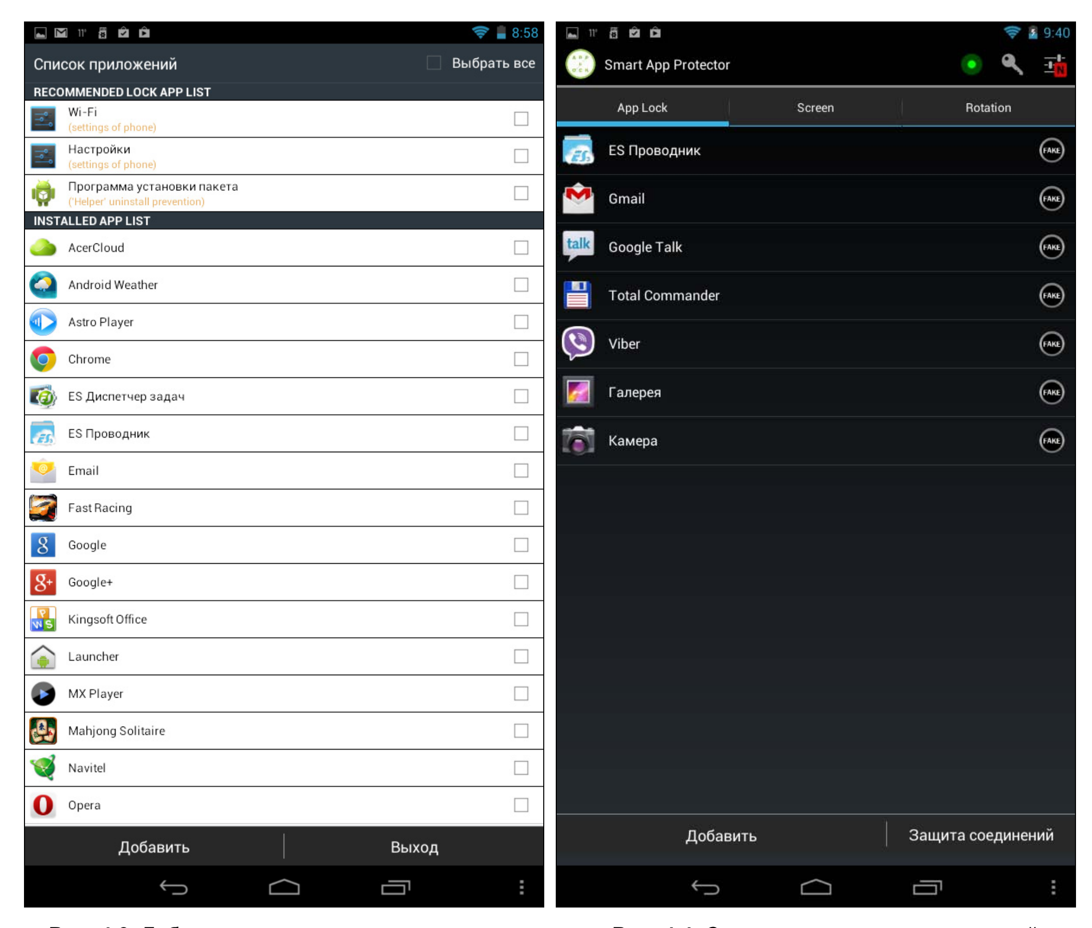


Рис. 4.3. Добавление приложения для защиты

Рис. 4.4. Список защищенных приложений

Вкладки **Screen** и **Rotation** тоже очень полезны. На них я добавил приложения Kingsoft Office, Chrome, Opera и Браузер. Можно на них добавить и приложения, с помощью которых вы читаете электронные книги. Мне не очень нравится, когда при чтении документов или просмотре веб-страниц экран гаснет или изменяет свою ориентацию при малейшем повороте устройства. Конечно, есть и общесистемные настройки, но меня устраивает возможность изменять параметры только для отдельных приложений, а не для всех установленных.

Сформировав список защищаемых приложений, просмотрите настройки программы, для чего нажмите кнопку с изображением буквы **N** в верхнем правом углу ее окна.

Основные настройки приложения App Lock (рис. 4.5) находятся в разделах **Блокировка экрана**, где можно определить, как будет выглядеть экран блокировки, и **Observer**, где можно задать параметры журналирования.

Перейдите в раздел **Блокировка экрана** — перед вами откроется экран блокировки (рис. 4.6).

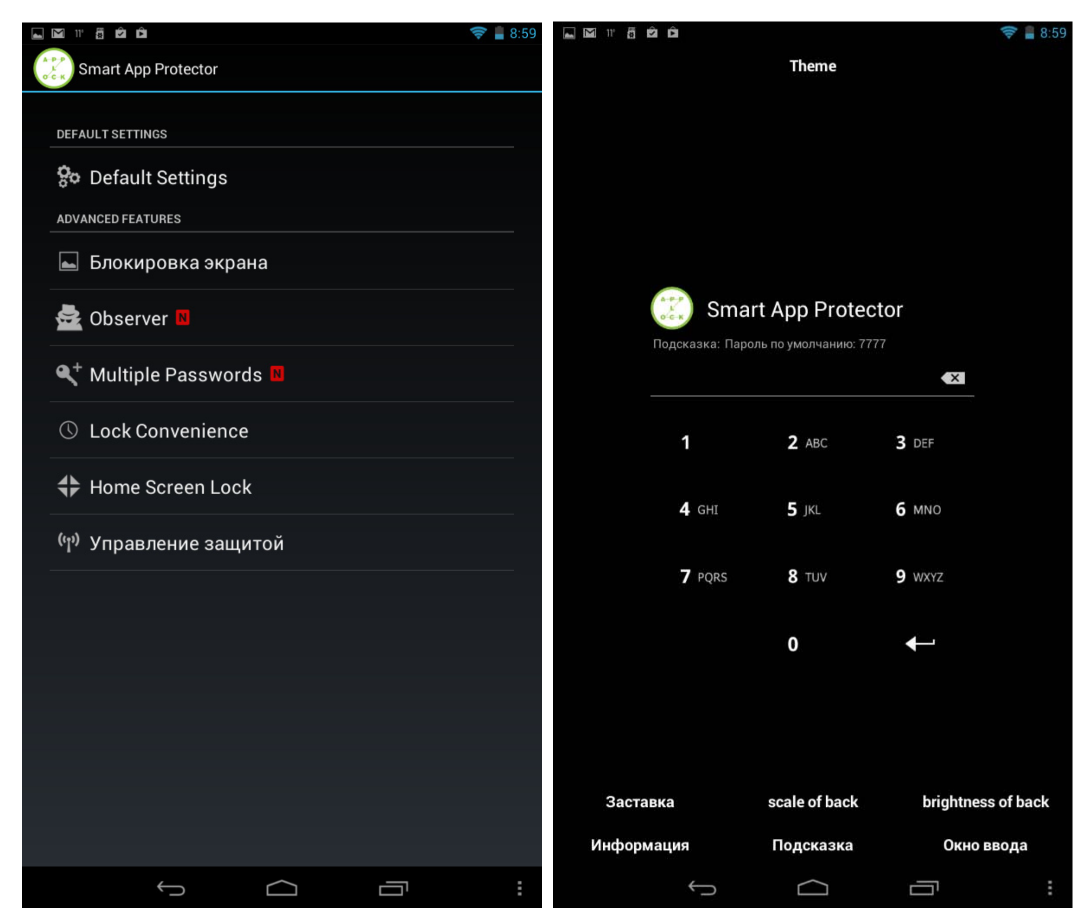


Рис. 4.5. Настройки приложения

Рис. 4.6. Так будет выглядеть экран блокировки

Нажмите кнопку **Заставка** — открывшаяся панель предоставляет возможность выбора заставки экрана блокировки (рис. 4.7). Здесь можно вообще отключить заставку или использовать системную, можно выбрать заставку из галереи (после выбора переключателя **Галерея** появится экран, позволяющий добавить одно или несколько изображений из галереи) или получить ее из камеры.

В разделе **Observer** настроек приложения (рис. 4.8) можно включить возможность журналирования неудачных попыток доступа к защищенным приложениям. Для этого установите переключатель в значение **ON**. Здесь же можно будет потом просмотреть журнал неудачных попыток доступа.

Теперь настало время установить пароль. Выйдите из настроек приложения и нажмите в правом верхнем углу его экрана кнопку установки пароля (с изображением ключа).

В открывшейся панели **Настройки защиты** (рис. 4.9) первым делом выберите команду **Варианты блокировки** и определите, какой будет использоваться пароль: цифры или графический ключ (рис. 4.10). Может, вариант **Жест** и кажется надежнее, но лично мне больше нравится вводить цифры.

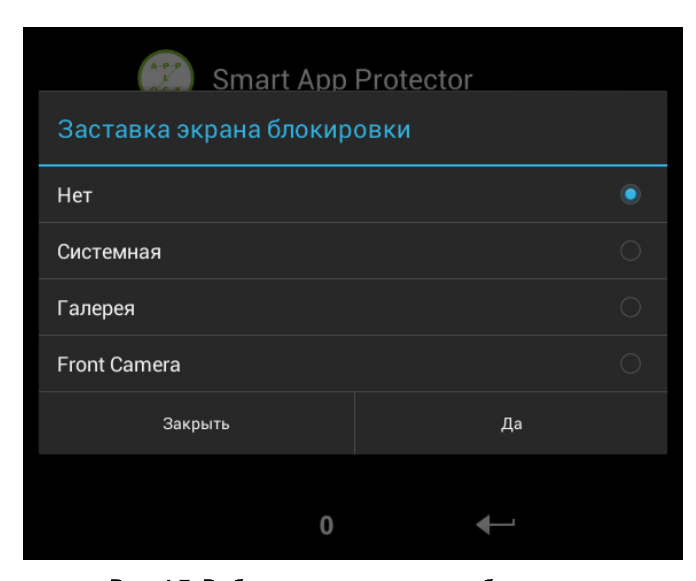


Рис. 4.7. Выбор заставки для экрана блокировки

9:00
Smart App Protector
OBSERVER
Observer
OFF
DESCRIPTION
Observer
Observer is monitoring a unlocking the success or failure. furthermore when unlock is failed, Observer can record picture/video and more.
LOG
There are no log

Рис. 4.8. Раздел **Observer**

9:00
Настройки защиты
LOCK TYPE
Варианты блокировки
НАСТРОЙКИ ЗАЩИТЫ
Пароль
Подсказка пароля
Подтверждение пароля
Используя эту функцию подтверждать правильно введенный пароль путем нажатия на клавишу "OK" не потребуется
Клавиатура
Номера клавиш набора пароля будут располагаться в случайном порядке
Removing Click Effect
Removing click effect when clicking password button
Тактильная связь
Подтверждение заданного рисунка и ввод пароля будут сопровождаться вибрацией

Рис. 4.9. Параметры пароля

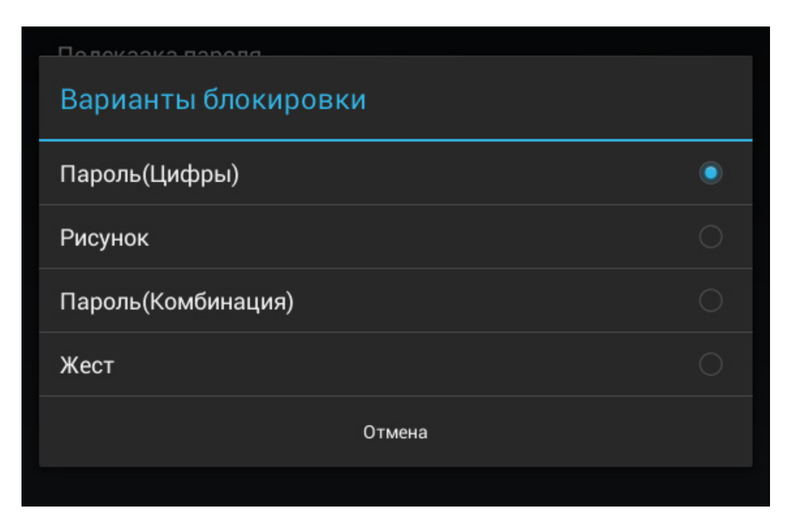


Рис. 4.10. Варианты блокировки

Вернитесь на экран, изображенный на рис. 4.9, и выберите команду **Пароль**, чтобы установить новый пароль, а затем измените, если сочтете нужным, подсказку пароля. Впрочем, чтобы сбить с толку злоумышленника, можно оставить подсказку по умолчанию.

Приложение почти готово к использованию. Но прежде хочу обратить ваше внимание на еще одну интересную его особенность. Перейдите к списку защищаемых приложений (см. рис. 4.4). Напротив каждого приложения вы увидите кнопку **FAKE**. Если режим FAKE активен, то при запуске приложения вместо приглашения ввести пароль будет отображено окно, имитирующее ошибку запуска приложения. Приложение не запустится, а злоумышленник решит, что просто произошел сбой. Чтобы запустить приложение, защищенное режимом FAKE, следует запустить App Lock и выключить режим FAKE, а уже затем запускать приложение. При запуске приложения с выключенным режимом FAKE будет запрошен пароль.

Итак, убедившись, что защита активна (зеленый кружок слева от кнопки установки пароля), приступим к проверке работы App Lock. Попробуйте запустить защищенное паролем приложение — последует приглашение ввести пароль (рис. 4.11). После ввода пароля приложение будет успешно запущено.

Теперь попробуйте запустить приложение с включенным режимом FAKE — вместо приглашения ввода пароля вы увидите сообщение о сбое запуска (рис. 4.12). Если просто нажать кнопку **Да**, то уведомление будет закрыто, а вот если нажать и удерживать эту кнопку, то появится стандартный экран блокировки, и приложение можно будет запустить после ввода пароля. Расчет здесь на то, что злоумышленник, ничего не подозревающий о работе App Lock, увидит сообщение о сбое приложения и просто нажмет кнопку **Да**, не вникая в написанное ниже предложение. Но даже если он его прочитает и будет удерживать кнопку **Да**, ему все равно придется ввести пароль.

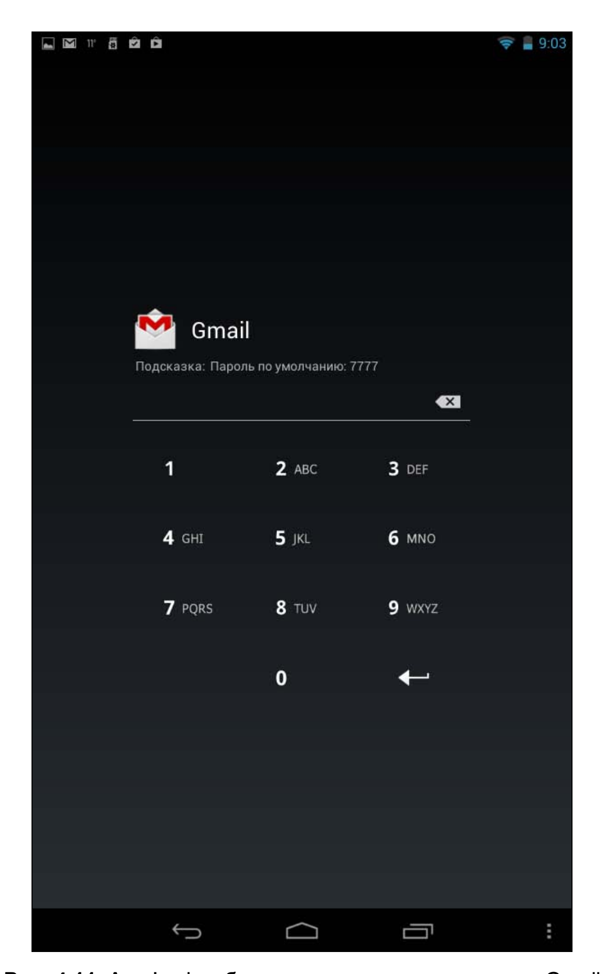


Рис. 4.11. App Lock заблокировал запуск приложения Gmail

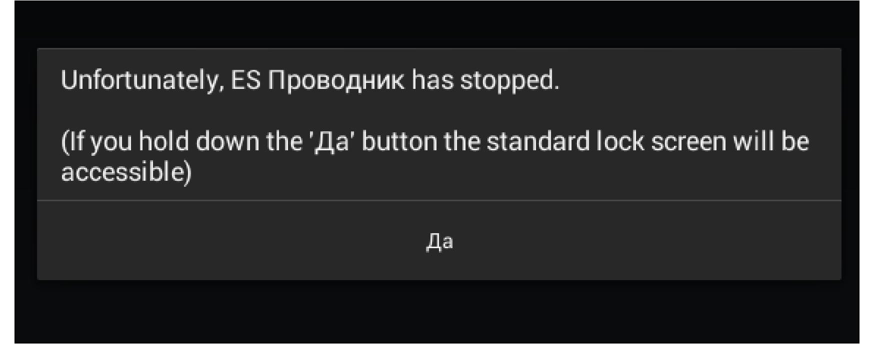


Рис. 4.12. Имитация сбоя приложения

4.3. Сокрытие папок из галереи

Приложение App Lock может просто запретить несанкционированный доступ к приложению Галерея, заблокировав его запуск паролем. Но представим, что у вас есть в галерее некоторые папки, которые вы не хотите никому показывать, и в то же время предпочитаете не использовать App Lock, поскольку оно требует пароля при каждом доступе к галерее, а это со временем начинает раздражать прежде всего вас.

Скрыть отдельные папки в галерее позволяет приложение Gallery Excluder. В Play Маркет вы его, к сожалению, не найдете. Скачать APK-файл этого приложения можно после бесплатной регистрации на сайте **4pda.ru** по ссылке:

http://4pda.ru/forum/index.php?showtopic=236864&st=20

> ***Примечание***
>
> Для установки APK-файла нужно разрешить установку из неизвестных источников. Для этого перейдите в раздел меню **Настройки | Безопасность** и установите флажок **Неизвестные источники**.

Использовать программу очень просто — запустите ее, выберите папки, которые нужно скрыть, и нажмите кнопку **Update media gallery** (рис. 4.13).

> ***Внимание!***
>
> Перед использованием этой программы на всякий случай сделайте резервную копию всех фотографий, музыки и видео (просто скопируйте их с устройства на компьютер). Некоторые пользователи сообщали, что использование этой программы приводило к уничтожению данных! Лишняя резервная копия никогда не помешает.

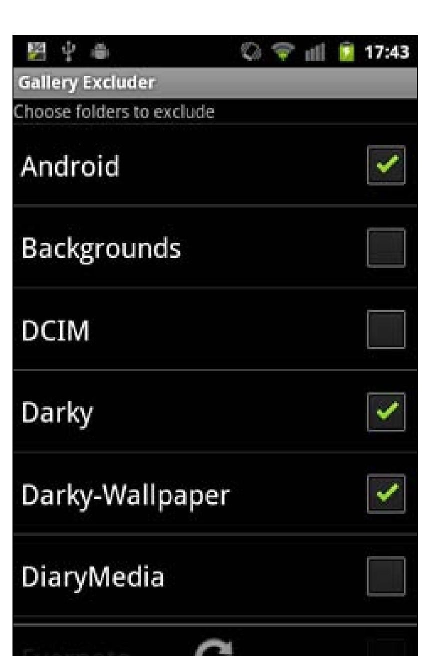


Рис. 4.13. Программа Gallery Excluder

4.4. Шифрование данных

4.4.1. Шифрование стандартными средствами

Операционная система Android (начиная с версии 2.3.4) поддерживает шифрование данных. Однако в отличие, например, от iOS, Android автоматически не шифрует данные, находящиеся на устройствах. Тем не менее шифрование можно легко включить, а как именно, мы сейчас и узнаем.

Шифрование устройства означает, что если телефон заблокирован, файлы на нем зашифрованы. При этом любые файлы, передаваемые с вашего телефона, напри-

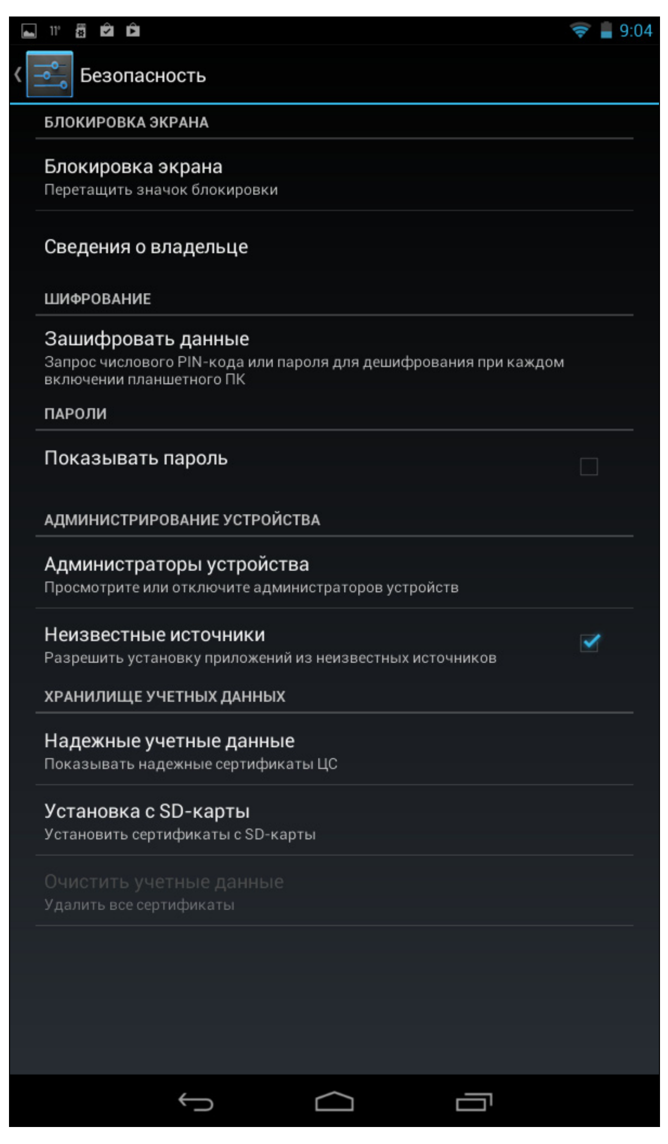


Рис. 4.14. Включение шифрования

мер, на компьютер или другой телефон, зашифрованы не будут. Сам процесс обмена данными (по Bluetooth, Wi-Fi и т. п.) тоже не зашифрован — для этого следует использовать методы, рассмотренные в *главе 6*. Но если вы скопируете файл с компьютера или другого телефона на ваш телефон, то он автоматически станет зашифрованным.

Для расшифровки файлов используется пароль, который вы вводите для разблокировки экрана. Если шифрование выключено, то этот пароль просто ограничивает доступ к экрану вашего телефона и ничего более полезного не делает. А вот если шифрование включено, то пароль — это ключ, служащий для дешифрования данных. И даже если злоумышленник найдет способ обхода экрана блокировки, ваши файлы все равно останутся зашифрованными.

Включить шифрование на Android-устройстве довольно-таки несложно — перейдите в **Настройки**, затем в раздел **Безопасность** (рис. 4.14) и выберите команду **Зашифровать данные** (или **Зашифровать устройство**).

Некоторые устройства поддерживают шифрование и внешней SD-карты — тогда среди опций появится команда **Зашифровать внешнюю карту** (рис. 4.15). В этом случае можно будет зашифровать и внешнюю карту памяти, что очень удобно — если кто-то извлечет карту памяти из вашего устройства, прочитать данные он не сможет.

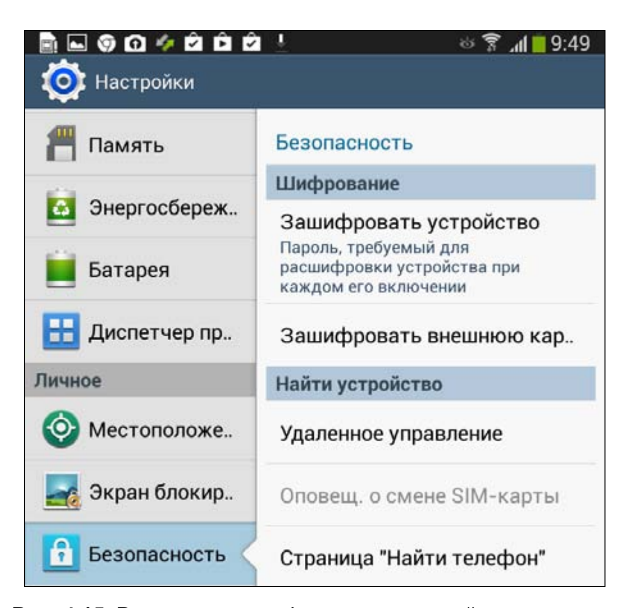


Рис. 4.15. Возможность шифрования внешней карты памяти

Однако если на вашем устройстве отсутствует возможность шифрования внешней карты, не спешите менять устройство. У вас есть два выхода: или хранить действительно важные данные на внутренней карте памяти (например, на моем устройстве внутренняя память составляет 8 Гбайт, что не мало даже по современным меркам), или же установить стороннюю программу шифрования.

4.4.2. Сторонние программы

Могу порекомендовать три программы шифрования данных (все они доступны на Play Маркет):

- LUKS Manager;
- EDS Lite;
- Cryptonite.

Программа LUKS Manager — старейшая программа шифрования файлов в Android. Она использует алгоритм шифрования AES, а само шифрование происходит «на лету». При этом поддерживаются файловые системы EXT2/4 и FAT32. Размер зашифрованного контейнера не ограничивается (разве что только размером памяти телефона).

К преимуществам программы можно отнести уже упомянутое шифрование «на лету» и простоту использования — работа с зашифрованными контейнерами осуществляется как с обычными папками.

Есть у программы и недостатки. В частности, она требует для своей работы прав root. Не поддерживает LUKS Manager и контейнеры TrueCrypt, которые стали сейчас де-факто практически стандартом. А жаль — очень удобно было бы создать на компьютере зашифрованный контейнер TrueCrypt, поместить его на флешку, а затем — при необходимости — на мобильный телефон, где можно было бы работать с ним как с обычной папкой.

Вторая программа — EDS Lite — хоть и молодая, но очень перспективная. Во-первых, для ее работы не нужны права root, что очень важно для многих пользователей. Во-вторых, программа поддерживает контейнеры TrueCrypt, а, как мы знаем, программа TrueCrypt сейчас работает на всех основных настольных платформах.

Но и эта программа не идеальна. Шифрование осуществляется не «на лету», и с зашифрованным контейнером нельзя работать как с обычной папкой. Однако программа содержит встроенный файловый менеджер, который поддерживает все операции над файлами. Например, вы можете создать зашифрованный контейнер в EDS Lite или в TrueCrypt, открыть его во встроенном файловом менеджере программы и скопировать в него все файлы, которые нужно зашифровать. Не очень, конечно, это удобно (нельзя использовать сторонние файловые менеджеры типа ES Проводник), но работать можно. Плохо здесь то, что остальные программы не поддерживают эти контейнеры. То есть, чтобы зашифровать документ, созданный в текстовом редакторе, вам придется явно поместить его в контейнер. Соответственно, чтобы прочитать этот документ, его надо будет явно скопировать из контейнера на карту памяти. Да, шифрования/дешифрования «на лету» очень не хватает этой программе. Зато она поддерживает два алгоритма шифрования: AES 256 и SHA-512. Далее мы программу EDS Lite рассмотрим подробно.

Программа Cryptonite совсем молода и находится еще на стадии тестирования. Использовать ее на практике я бы пока не стал, зато она поддерживает облачные диски, что весьма немаловажно сейчас, когда пошла мода на облачные технологии.

Существенный недостаток этой программы — то, что она требует от ядра Android поддержки Kernel FUSE, а такая поддержка есть не в каждом телефоне.

Итак, вернемся к программе EDS Lite. Сейчас она для нас наиболее приемлема, поскольку для работы LUKS Manager нужны права root, а Cryptonite пока лучше не использовать, но иметь ее в виду следует — через некоторое время, если разработчики ее не забросят, это будет очень перспективный проект.

Суть работы программы EDS Lite состоит в том, что она создает зашифрованный контейнер. По сути, это один большой файл (размер файла задается при создании контейнера), в который вы можете поместить другие файлы. Такой контейнер можно сравнить с запароленным архивом с нулевой степенью сжатия. Конечно, алгоритмы шифрования здесь более совершенны по сравнению с архиватором, но приведенное сравнение облегчает понимание понятия «контейнер».

Когда вы запускаете программу впервые, список контейнеров пуст (рис. 4.16).

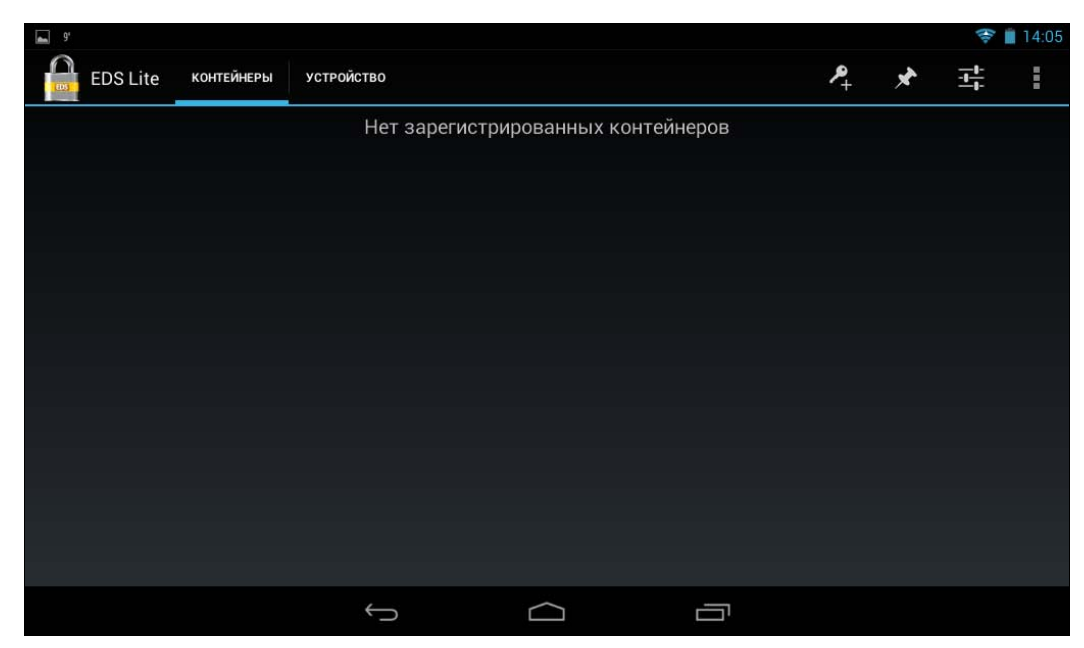


Рис. 4.16. Список контейнеров пуст

Для создания нового контейнера нажмите кнопку с изображением ключа со знаком +. На открывшейся панели (рис. 4.17) вы сможете ввести параметры контейнера, а именно:

- путь к файлу контейнера — лучше создавать контейнеры на внешней SD-карте. Даже в случае выхода устройства из строя, внешнюю SD-карту можно будет извлечь и прочитать данные. Да и места на внешней карте, как правило, больше;
- пароль — программа, к сожалению, допускает использование простых паролей. Ради интереса я ввел пароль `qwerty`, и программа его «проглотила». Не предусмотрено и поле подтверждения пароля, поэтому будьте внимательны при вводе пароля, чтобы не допустить ошибку;

- размер контейнера — определите максимальный размер, который сможет занимать файл, указанный в первом параметре. На рис. 4.17 показано, что создается контейнер размером 2 Мбайт. Это значение по умолчанию, и оно очень мало. Столь маленький контейнер можно создать или чтобы научиться работать с программой, или если вам нужно хранить в контейнере только лишь текстовые документы, которые не занимают много места. Определите размер контейнера, исходя из своих потребностей. Кому-то и 20 Мбайт будет достаточно, а кому-то и 2 Гбайт мало.

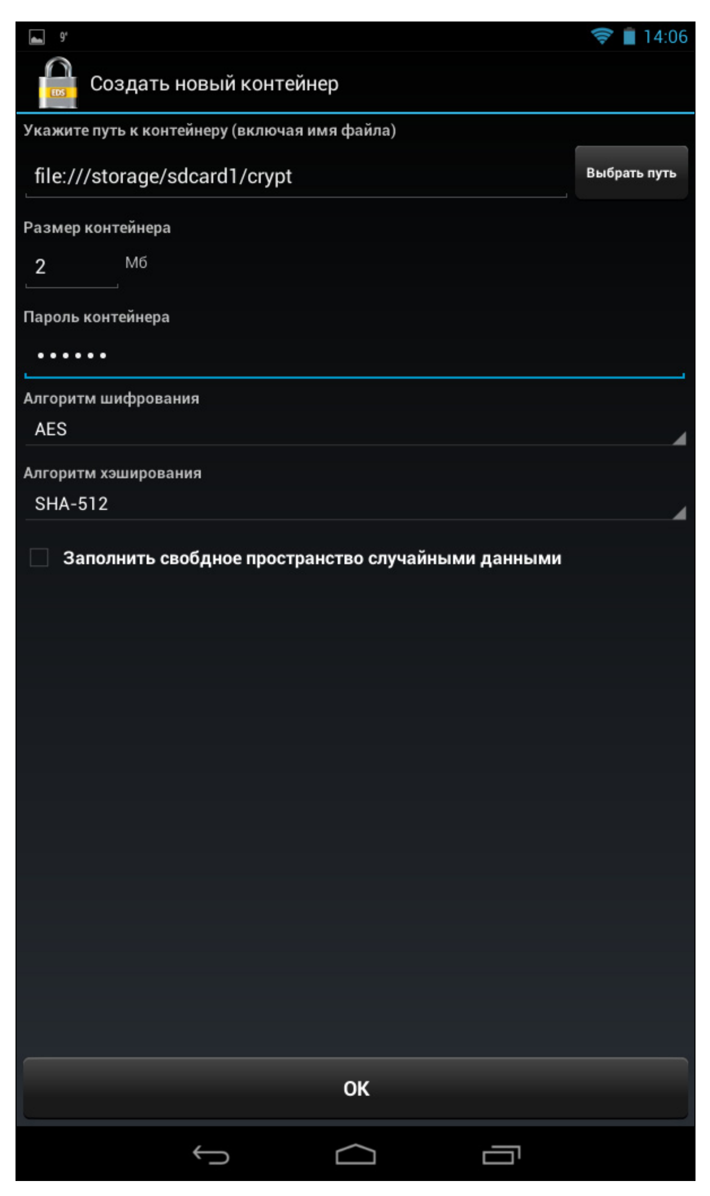


Рис. 4.17. Создание контейнера

Остальные параметры можно оставить без изменения. Нажмите кнопку **OK** для создания контейнера. После этого вы увидите свой контейнер в списке контейнеров (рис. 4.18). Выберите созданный контейнер — появится панель ввода пароля.

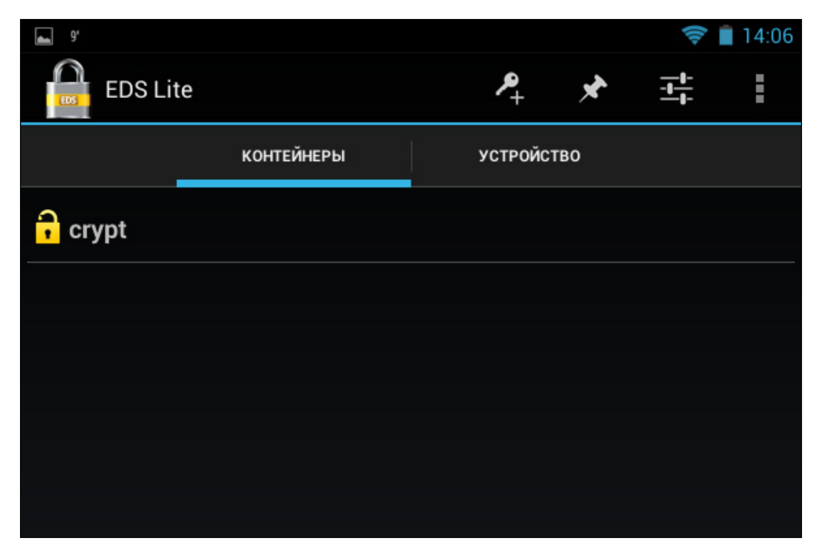


Рис. 4.18. Созданный контейнер

Иллюстрации работы с паролем

Дальнейшие иллюстрации работы с паролем сделать невозможно, поскольку программа блокирует создание снимков экрана — нельзя «сфотографировать» ни окно ввода пароля, ни содержимое контейнера.

В открытом контейнере вы увидите двухпанельный файловый менеджер. Используйте его для помещения в контейнер нужных файлов — они при этом будут зашифрованы. Незашифрованные версии файлов с вашей SD-карты, разумеется, следует удалить — иначе, какой смысл в создании контейнера?

В целом, программа EDS Lite довольно удобна. Да, она не позволяет работать с зашифрованными файлами через сторонние файловые менеджеры, но зато не требует прав root. И, в отличие от стандартных средств шифрования, позволяет зашифровать только те файлы, которые нужно, а не все устройство или не всю SD-карту.

В следующей главе мы поговорим о выборе антивируса для вашего Android-устройства, а в *главе 6* — о шифровании передаваемых по сети данных. *Глава 11* также тесно связана с шифрованием данных — в ней мы создадим «скрытый» телефон внутри обычного. Но даже если вы этим сейчас заинтересовались, все равно не спешите читать *главу 11*, прочитайте предварительно хотя бы *главу 10*.



ГЛАВА 5

Антивирус для Android

5.1. Нужен ли антивирус в Android?

Устройства на базе Android становятся все популярнее. По сути, у Android в общем-то и нет конкурентов. Устройства на базе iOS сто́ят относительно дорого и не каждому по карману, а устройства на базе Windows Phone покупать не спешат — хочется, чтобы хотя бы смартфон работал надежно. Конечно, последние версии Windows функционируют достаточно стабильно, но осадок прошлых времен остался. Устройства на базе Bada OS (собственная разработка Samsung) постепенно вытесняются устройствами на базе Android даже внутри самой компании Samsung — по сути, на Bada OS остались лишь самые дешевые устройства.

Популярность устройств на базе Android понятна: небольшая цена, открытость, возможность настраивать операционную систему смартфона на любой вкус и цвет, огромное количество бесплатных приложений. Пользователю, купившему смартфон, не придется выложить еще столько же за приложения для него (как в случае с устройствами на iOS).

Но популярность Android-устройств и такая их распространенность открывают огромное поле деятельности для различных злоумышленников. Только за 2013 год количество вредоносных программ для Android увеличилось на 180 % — до 519 тысяч[1] (!). Отсюда и значительная вероятность установить одну из таких программ. Поэтому антивирус на Android является практической необходимостью.

Не следует также думать, что если вы загружаете программы только из Play Маркет, то останетесь в безопасности. Вирус DroidDream как раз и распространялся через официальный сайт Google Play Маркет, и при этом все пользователи, загрузившие содержащие его приложения, были уверены в том, что они безопасны. Конечно, Google вскоре удалила содержащие вирус приложения, но это наталкивает на мысль, что Google не слишком усердно проверяет на предмет вредоносного кода приложения, публикуемые на Play Маркет сторонними программистами.

---

[1] См. **http://hi-tech.mail.ru/news/android-malware-180.html**.

Итак, нужен ли антивирус на смартфоне? Многие пользователи исходят из опыта работы с настольными системами, где антивирус просто необходим, и устанавливают антивирус на Android-устройства. Причем стараются, чтобы на смартфоне стоял такой же антивирус, что и на настольном компьютере. Например, если человек использует Dr.Web на ноутбуке или стационарном компьютере, то он стремится установить Dr.Web и на свой смартфон/планшет.

Да и в Сети можно найти много информации о том, что вирусы, трояны и другое вредоносное программное обеспечение поселяется на мобильные телефоны, в том числе и под управлением Android. Вирусы проникают даже на Play Маркет, а на самом Play Маркет антивирусные программы являются чуть ли не самыми популярными по количеству загрузок.

Все это создает впечатление, что у Android все плохо и с безопасностью, и с вирусами. Однако на самом деле это не так, поскольку Android самостоятельно проверяет устройство на наличие вредоносных программ. Другими словами, функции антивируса уже встроены в саму операционную систему.

Вот, что может делать Android без установки стороннего антивируса:

- приложения на Google Play Маркет проверяются на вирусы при загрузке. Если приложение является вирусом или содержит вредоносный код, то оно не будет загружено на Google Play Маркет, и вы просто не сможете его скачать и установить;
- если же каким-либо образом на Play Маркет появится вредоносное приложение (были и такие ситуации), и вы его уже установили, Google может удалить его с вашего телефона;
- начиная с версии 4.2, ОС Android может проверять сторонние приложения (из неизвестных источников) на наличие вирусов. При первой установке стороннего приложения на Android 4.2 пользователю будет задан вопрос, нужно ли проверить приложение на наличие вредоносного кода;
- Android 4.2 автоматически блокирует силами операционной системы отправку платных SMS, запрещена также фоновая отправка SMS на короткие номера, что часто используют трояны. При попытке приложения отправить такое SMS вы получите соответствующее уведомление;
- Android ограничивает опасные возможности приложений — так, приложения не могут работать в фоновом режиме и записывать каждое нажатие клавиши, что исключает наличие в Android «клавиатурных» (клавиатура-то виртуальная) шпионов. Кроме того, при установке приложения вы увидите все разрешения, необходимые программе.

Как видите, список защитных свойств Android довольно впечатляет. И все это умеет сама операционная система без антивирусов. Так что, если следовать рекомендациям, приведенным далее в *разд. 5.3*, то антивирус, по сути, особо и не нужен.

Устройства под управлением Android 4.2 защищены лучше. А вот на более ранние версии следует, все же, для верности установить антивирус.

5.2. Что представляют собой вирусы для Android?

Как мы уже отметили, операционная система Android 4.2 и сама неплохо защищена от вредоносного кода. Защита же предыдущих версий осуществляется через Google Play Маркет — при загрузке туда приложения проверяются на наличие вредоносного кода, поэтому, если вы загружаете приложения через Play Маркет, вы уже *относительно* защищены, а вот загружая приложения из других источников, подвергаете себя огромному риску.

Что представляют собой вирусы для Android? Более 50 % всех вирусов — это код FakeInstaller, вредоносная программа, замаскированная под полезное приложение. Такое себе подобие трояна для Android. Будучи загружен на устройство, вредоносный код начинает рассылать с него платные SMS. Понятно, что вы об этом узнаете только тогда, когда ваш счет опустеет. Как уже было отмечено, Android 4.2 от этого защищена.

Относительность защиты приложений, загружаемых через Google Play Маркет, обусловлена тем, что стопроцентной чистоты приложений этот сервис, все же, не гарантирует. По статистике вредоносное программное обеспечение, встречающееся на Google Play Маркет, составляет 0,5 % от общего числа содержащихся там программ. Это совсем немного, но вы должны знать, что и через Google Play Маркет можно загрузить вирус.

По сути, вероятность получить на Android-устройство вирус весьма мала. Однако если вы любите экспериментировать и часто загружаете приложения из неизвестных источников, то лучше установить-таки антивирус. А какой именно, будет подсказано в *разд. 5.4*.

Не следует также забывать, что антивирус немного снижает производительность устройства, что особенно почувствуют владельцы старых смартфонов, которым придется выбирать: или производительность, или безопасность. Поэтому далее приводятся простые рекомендации, соблюдение которых снижает вероятность заражения вирусом практически до нуля.

5.3. Общие рекомендации

Как уберечься от вирусов? Существуют несколько простых рекомендаций, выполнение которых существенно снизит риск заражения вирусом вашего смартфона. Стопроцентной гарантии эти рекомендации, само собой, дать не могут, но и хуже однозначно не будет.

- **Загружайте приложения только из надежных источников** (подробно это мы обсуждали в *главе 2*). Лучше всего, конечно, загружать приложения из Play Маркет. Хотя, как показывает ситуация с DroidDream, эта рекомендация не может дать полной гарантии безопасности, но, все же, вероятность получить приложение с вирусом из Play Маркет значительно ниже, чем из других источников. В Play Маркет имеются все необходимые приложения, но некоторыми пользова-

телями движет желание сэкономить. Да, на Play Маркет не все приложения бесплатные, и с некоторых других сайтов можно скачать платные приложения со взломанной защитой абсолютно бесплатно. Но где гарантия, что человек, взломавший защиту приложения, не внедрил в него свой вредоносный код? Правильно, такую гарантию никто дать не может. Здесь уже нужно выбирать, что важнее: или здоровье смартфона, или возможная экономия. Про морально-этические нормы я уже вообще молчу.

- **Устанавливайте обновления операционной системы**. Google регулярно выпускает обновления Android, позволяющие «залатать» дыры в безопасности. Не ждите, пока какая-нибудь программа воспользуется одной из таких дыр — потом будете жалеть, что вовремя не обновили операционную систему.
- **Ограничьте использование бесплатного Wi-Fi**. Лучше не передавать пароли через бесплатный Wi-Fi в публичных местах — помните, что передаваемая информация может быть перехвачена. Эта рекомендация означает, что при подключении к Интернету по бесплатной публичной сети Wi-Fi не следует проверять и отправлять почту, заходить на сайты социальных сетей и, вообще, нужно прекратить любую деятельность, связанную с передачей каких-либо данных, вводом паролей и работой с важной информацией. Существенно повысить уровень безопасности в таких сетях может организация VPN-соединения (см. об этом *главу 6*), т. к. передаваемые при этом данные (в том числе и пароли) будут зашифрованы.
- **Серьезно относитесь к паролям**. Не используйте простые пароли вроде 123456, 1111, qwerty и т. п. Простые пароли очень легко подбираются специальными программами, поэтому лучше придумать какую-то более сложную комбинацию символов. В такой комбинации должны присутствовать символы обоих регистров (строчные и прописные), цифры и, по возможности, любые другие допустимые символы. Вот пример хорошего пароля: `VhZ,89sE`. В идеале для каждого аккаунта (Google, почты, Skype, странички в социальной сети) должен существовать свой пароль. Тогда, если один из аккаунтов будет взломан, остальные останутся в безопасности. Самый сложный пароль следует задать для электронной почты, поскольку через нее обычно осуществляется восстановление паролей других сетевых служб, и если злоумышленник получит пароль от вашего почтового ящика, то сможет «восстановить» пароли и от других сервисов (от социальной сети, от Skype и т. п.). Если хранить в собственной памяти все пароли не получается, используйте специальные программы типа KeePass, но, на мой личный, конечно, взгляд, лучше стараться нужные пароли просто помнить.

5.4. Выбор и установка антивируса

Проще всего написать «установите антивирус». Но какой именно антивирус? Когда заходишь на Play Маркет и вводишь запрос `антивирус`, поисковик находит столько вариантов, что глаза разбегаются. Какой из них установить? Дело-то не просто в установке какого-то там антивируса, надо, чтобы и толк от его применения был.

К тому же хочется, чтобы антивирус был бесплатным. Все-таки Android — это не iOS, и не всегда у пользователя Android есть желание или возможность покупать приложения за деньги.

Итак, рассмотрим несколько вариантов.

- Dr.Web v.7 Антивирус Light — простой антивирус, обеспечивающий только базовую защиту. Много чего умеет, но все же не обеспечивает комплексной защиты от вирусов и прочих угроз. Зато полностью бесплатный.
- Dr.Web v.9 Антивирус — обеспечивает полноценную защиту от вирусов и прочих угроз. Довольно неплохой антивирус, но — увы — платный. Первые 15 дней его можно использовать бесплатно, а потом надо либо удалить, либо купить лицензию на год. Можно купить лицензию и на 2 года, но без технической поддержки. Это означает, что каждые 1 или 2 года за антивирус нужно будет платить. Самое интересное, что приложение это работает нестабильно и периодически аварийно завершает работу. Если вы фанат Dr.Web, то или используйте бесплатную Ligth-версию, или установите какой-нибудь другой антивирус. Платить деньги за «сырое» приложение не вижу смысла.
- Kaspersky Internet Security — еще один платный антивирус от известного разработчика. Увы, качество тоже хромает. У многих пользователей (особенно на устройствах Samsung Galaxy S) наблюдается проблема с обрывом Wi-Fi при работающем антивирусе. На данный момент (13 апреля 2014 года) проблема эта так и не устранена. Возможно, написанное здесь послужит толчком для разработчиков, и они все же исправят свои ошибки, а пока это приложение не стоит запрашиваемых денег.
- AVG Mobile — бесплатный и очень эффективный антивирус. Регулярно обновляется, быстро работает и зарекомендовал себя с хорошей стороны. Если же нужна более надежная защита, можно установить профессиональную платную версию AVG PRO, но, как показывает практика, бесплатной версии вполне достаточно.
- avast! Mobile Security для Android — приложение очень неплохое, но требует прав root. О том, как получить права root, будет рассказано в *главе 10*, но на вашем месте я бы поискал другой антивирус, работающий без полномочий root.

В Play Маркет содержится более 100 различных антивирусов, и этот список мог бы быть весьма длинным. Но продолжать его никак не хочется, как и тестировать все возможные антивирусы. Поэтому в нашем небольшом списке всего пять вариантов — это самые известные антивирусы, знакомые нам еще с настольных платформ. Лучший, на мой взгляд, антивирус — AVG Mobile (бесплатная версия). Это приложение выигрывает на фоне конкурентов стабильной и быстрой работой, регулярными обновлениями и стоимостью (вернее, ее отсутствием). Если же AVG Mobile вам чем-то не понравился, можно попытаться установить Dr.Web v.7 Антивирус Light — приложение хоть и не обеспечивает полной защиты, однако работает стабильно. Во всяком случае, оно бесплатно, и с ним не возникнет неприятной ситуации, когда вы и деньги заплатили, и все равно поймали вирус, что нередко происходит с некоторыми антивирусными программами.

Помните, что антивирус — не панацея и не гарантирует полной безопасности. Если вы скачали пиратскую версию игры, то приготовьтесь, что получите не то, что ожидали, даже если установили самый лучший антивирус. В лучшем случае приложение просто не запустится, а в худшем антивирус не сможет распознать вредоносный код.

Еще раз напомню, что антивирусы снижают производительность, и на очень слабых устройствах проще придерживаться рекомендаций из *разд. 5.3*, чем «душить» и без того «чахлое» устройство антивирусом.

В следующей главе мы поговорим о защите передаваемых по сети данных. Будет показано, как настроить в Android VPN-соединение, мы также рассмотрим несколько скандальный, но очень эффективный проект Tor. Пойдет речь и о проекте I2P, который можно рассматривать как альтернативу Tor, но не как его замену.



ГЛАВА 6

Защита передаваемых по сети данных. Анонимность при работе в Интернете

6.1. VPN-соединение и Android

6.1.1. Зачем нужно в Android VPN-соединение?

В *главе 4* мы рассмотрели защиту и шифрование данных, находящихся на самом телефоне, а сейчас речь пойдет о защите данных, передаваемых по сети. Надо иметь в виду, что все данные (за исключением передаваемых по безопасным HTTPS-соединениям) пересылаются по сети в открытом виде. И когда вы передаете по сети какие-либо данные (просматриваете веб-страницы, вводите пароли, получаете и отправляете почту, заполняете на сайтах те или иные формы, получаете и пересылаете файлы), они могут быть перехвачены. Но кем? Да кем угодно, в этом заинтересованным.

Если вы подключаетесь к Интернету по Wi-Fi, то данные могут быть перехвачены на отрезке телефон–маршрутизатор Wi-Fi, их могут перехватить и на самом маршрутизаторе Wi-Fi, кроме того, данные перехватывает и анализирует оборудование провайдера, предоставляющего доступ к Интернету владельцу беспроводного маршрутизатора. Другими словами, даже предположить сложно, в каком именно месте ваши данные могут быть перехвачены.

При подключении к Интернету через сеть мобильного оператора на участке от телефона до базовой станции перехват данных организовать не в пример сложнее. Но, ясное дело, их вполне может перехватывать сам мобильный оператор — точнее, он их может запросто записывать, поскольку ваш трафик и так проходит через его оборудование. Реально записывает он ваш трафик или нет — никто не знает, но то, что фиксируются посещенные вами сайты и другая ваша сетевая активность: IP-адреса узлов, к которым вы подключались, — например, почтовых, FTP-серверов и т. п. — это точно.

Как защитить себя от такого безобразия? Выход один — использование VPN (Virtual Private Network, виртуальная частная сеть). Объяснять здесь, что такое VPN и откуда она взялась, я не стану. Достаточно отметить, что через VPN-соединение

весь обмен данными происходит в зашифрованном виде, и ни «перехватчик» в локальной сети (при подключении Wi-Fi), ни интернет-провайдер, ни мобильный оператор перехватить ваши данные не смогут. Точнее, перехватить-то они как раз смогут, но вот расшифровать — вряд ли...

Для организации VPN-соединения вам нужно найти подходящий VPN-сервис и подключиться к нему. Тогда ваши данные будут в зашифрованном виде отправляться на VPN-сервер, а оттуда пересылаться тому узлу, с которым вы фактически желаете работать. Провайдер же увидит только обращение к VPN-сервису и то, что вы передаете какие-то данные. Но определить, куда фактически идут дальше данные и что именно вы отправляете, он не может.

Проблема здесь в том, что хорошие и быстрые VPN-сервисы — платные, хоть и плата эта невелика (порядка $40 в год). Далее мы поговорим о выборе VPN-сервиса.

6.1.2. Выбор VPN-сервиса

Сравнение популярных VPN-сервисов можно найти в Интернете, здесь же мы рассмотрим несколько тех из них, на которые вам следует обратить внимание.

Private Internet Access

Private Internet Access (**http://privateinternetaccess.com/**) — один из старейших VPN-сервисов, предоставляющих в сети услуги анонимизации. Кроме привычных услуг (анонимизация, обеспечение конфиденциальности, шифрование) сервис предоставляет также защиту от изменения DNS-серверов (DNS leak protection). При этом у пользователя имеется возможность подключить к сервису до трех устройств одновременно.

Первое, на что пользователи обращают внимание при выборе VPN-сервиса (да и всего прочего в большинстве случаев), — это тарифные планы. Тарифных планов у сервиса Private Internet Access три:

- можно платить каждый месяц по $6,95;
- можно платить раз в полгода по $35,95 (при этом стоимость одного месяца снижается до $5,99);
- можно платить один раз в год $39,95 (при этом стоимость одного месяца составит всего $3,33).

Ясное дело, что последний тарифный план — самый экономный. Сервис предоставляет также бесплатный тестовый доступ сроком на 7 дней.

Все тарифные планы обеспечивают одинаковые сервисы и возможность использовать различные типы подключений (OpenVPN, PPTP и IPSec), неограниченный трафик (т. е. оплаченный тарифный план — это окончательная стоимость, и более ни за что платить не придется) и возможность выбрать шлюз в любой стране, где работает сервис, а именно: в США, Великобритании, Германии, Канаде, Франции, Швеции, Швейцарии, Нидерландах, Гонконге (Китайская Народная Республика), Румынии.

Иностранный IP-адрес

Возможность выбрать страну означает, что у вас будет IP-адрес этой страны. VPN-сервисы этим очень удобны — помню, однажды для доступа к некоему автомобильному сайту (база данных запчастей для «мерседеса») мне понадобился немецкий IP-адрес, а получить его можно только таким образом или через Tor (см. далее). С другой стороны, некоторые российские сайты ограничивают доступ для «иностранцев», поэтому зайти на такие сайты с использованием VPN не получится.

Техническая поддержка сервиса осуществляется по e-mail и через чат сайта. На самом же сайте сервиса имеется весьма обширный список часто задаваемых вопросов.

Сервис предоставляет собственные VPN-клиенты для Android. VPN-клиент для Android 4.*x* можно установить с Play Маркет по ссылке:

https://play.google.com/store/apps/details?id=com.privateinternetaccess.android

Для более старых версий Android (2.*x* и 3.*x*) клиент можно скачать с сайта VPN-сервиса по ссылке:

https://www.privateinternetaccess.com/pages/client-support/#android_ipsec_l2tp

Конечно, как и у всего на свете, у сервиса Private Internet Access имеются недостатки:

- не предоставляется список всех точек присутствия с указанием IP-адресов шлюзов — т. е., при выборе точки присутствия вы не будете знать, какой IP-адрес у вас окажется «на выходе». Проверить IP-адрес можно только после подключения к той или иной точке присутствия, для чего нужно будет зайти на сайт **http://www.geoiptool.com/ru/** или подобный;
- не предоставляется информация о загруженности каналов передачи данных и серверов;
- если пользователь нарушит чьи-либо авторские права, информация о нем будет отправлена непосредственно правообладателю — большинство серверов сервиса находится в США, и он следует акту Digital Millennium Copyright Act (DMCA);
- небольшое количество точек присутствия — всего 10 стран, хотя шлюзов гораздо больше, но многие из них расположены в разных районах США, Канады и Великобритании.

StrongVPN

Сервис StrongVPN (**http://strongvpn.com/**) тоже родом из США. Он является одним из первых провайдеров, предоставляющих услуги шифрования передаваемой информации.

Сайт сервиса предлагает много разных и довольно гибких тарифных планов, там же вы найдете и огромное количество документации, с помощью которой сможете настроить любое устройство, поддерживающее VPN.

Самый дешевый тарифный план — «облегченный» PPTP-доступ сроком на 3 месяца — обойдется пользователю в $21. Стоимость чуть выше, чем у сервиса Private Internet Access, хотя можно счесть, что практически такая же. Тестового периода

нет, но компания гарантирует возврат денег (moneyback), если у вас не получилось настроить или использовать VPN-подключение в течение 7 дней, независимо от выбранного тарифного плана.

Как и предыдущий сервис, StrongVPN обеспечивает возможность использовать различные типы подключений: OpenVPN, L2TP/IPSec и PPTP. Если что-то не получится, к вашим услугам круглосуточная поддержка (в чате, по e-mail, по телефону и Skype). Да, поддержка, как и у сервиса Private Internet Access, осуществляется на английском языке — что ж тут поделаешь, язык международного общения хоть в малых объемах, но знать все же требуется...

Огромный недостаток сервиса StrongVPN — то, что он полностью работает в рамках законов США, т. е. компания сохраняет всю информацию о пользователе, включая журналы доступа, персональную информацию, время подключения и даже IP-адрес в его внутренней сети за маршрутизатором. Если вам нужна анонимность и конфиденциальность, то сервис StrongVPN — явно не ваш выбор.

К недостаткам этого сервиса можно отнести и то, что у нет никакого клиентского программного обеспечения, т. е. пользователю придется настраивать свое устройство самостоятельно.

HideMyAss (HMA)

Штаб-квартира сервиса с не очень приличным названием находится в Англии (**http://hidemyass.com/**), но точки присутствия имеются в 61 стране мира (всего насчитывается 448 серверов).

Сервис предоставляет огромное число дополнительных сервисов, однако описание большинства из них не соответствует тому, что указано на сайте. Стоимость же услуг зашкаливает — за один месяц нужно заплатить $11,52, впрочем за полгода цена более приятная — $39,99 (или $6,67 в месяц). Тестового периода нет, но есть гарантия возврата средства в течение 30 дней с момента оплаты.

Сервисом предоставляется поддержка протоколов L2TP, OpenVPN, PPTP (IPSec не поддерживается). Сам сервис рекомендует использовать протокол OpenVPN.

Недостатки у этого сервиса тоже есть и существенные. В частности, он собирает много информации о деятельности пользователя и хранит ее два года. Так что название сервиса не совсем соответствует действительности. К недостаткам также можно отнести уже упомянутое отсутствие возможности использования протокола IPSec и отсутствие клиентов для Android.

IPVanish VPN

Штаб-квартира этого сервиса (**https://www.ipvanish.com/**) находится в США. Это еще один крупный американский VPN-провайдер.

Тарифных планов у сервиса три: или каждый месяц по $10, или каждые три месяца по $26,99, или раз в год, но $77,99. Трафик (вне зависимости от выбранного тарифного плана) не ограничивается.

Точек присутствия не так много, как у сервиса HMA, но и не мало. Серверы сервиса находятся в США, Канаде, Великобритании, Франции, Японии, Малайзии, Венгрии, Нидерландах, Южной Африке, Испании, Швеции и Южной Корее.

Сервис IPVanish VPN тоже собирает информацию о пользователях и работает в рамках акта DMCA Copyright Policy. Однако на сайте сказано, что собирается только самая необходимая информация, но какая именно — не сообщается.

Сервис поддерживает протоколы PPTP, L2TP и OpenVPN. Протокол IPSec не поддерживается и в этом случае.

Недостатки сервиса такие же, как в предыдущем случае: запись информации о пользователе и отсутствие возможности использования IPSec. Недостаток же сугубо этого сервиса — не очень адекватная служба поддержки, ответа которой нужно ждать часами.

ExpressVPN

Молодой VPN-провайдер (**https://www.express-vpn.com/**) с довольно высокими ценами. За один месяц нужно будет отдать $12,95 или за год — $99,95. Компания гарантирует возврат денег в течение 30 дней, если у вас возникли проблемы с использованием сервиса.

Точек присутствия тоже немного: США, Великобритания, Нидерланды, Канада, Германия, Гонконг. Пользователь может выбрать любой из сервисов и переключаться между ними.

К достоинствам сервиса ExpressVPN можно отнести удобное программное обеспечение для Windows, Linux, Mac OS и, конечно же, для Android. Поддерживаются только протоколы PPTP и OpenVPN.

Недостатки:

- мало точек присутствия;
- наличие жалоб на службу технической поддержки от пользователей (в Интернете много негативных отзывов от пользователей);
- отсутствие поддержки протоколов L2TP и IPsec;
- компания собирает и хранит много информации о пользователе, которая может быть передана третьим лицам в соответствии с законодательством США.

VPN Shield

Сервис VPN Shield (**http://www.vpnshieldapp.com/ru**) отличается очень демократичными ценами. Так, неделя доступа обойдется всего в $0,99, а месяц — в $3,99. Подписку на 3 месяца можно купить за $9,99, а на год — всего за $29,99. Это самый дешевый VPN-сервис.

Компания находится в Люксембурге, а это означает, что законодательство США на нее не распространяется, но у компании есть серверы в США, Германии, Англии, Нидерландах и Китае.

Сервис поддерживает все популярные протоколы: PPTP, L2TP, IPsec, OpenVPN.

К недостаткам сервиса VPN Shield можно отнести службу поддержки, работающую только через e-mail, — не очень оперативное средство связи.

Зато компания не собирает (а если и собирает, то явно об этом не сказано) информацию о пользователях.

С Play Маркет можно скачать соответствующий Android-клиент, что сильно упростит настройку вашего устройства для работы с этим сервисом.

На мой взгляд, последний рассмотренный сервис представляет собой практически идеальный вариант. Какую-то информацию о пользователе он, конечно же, собирает, но не такую подробную, как другие сервисы. К тому же сервис предоставляет удобный Android-клиент, а учитывая стоимость предоставляемых услуг, он вовсе вне конкуренции.

6.1.3. Настройка встроенного VPN-клиента Android

Если сервис предоставляет собственный VPN-клиент, используйте его — тогда вам ничего не придется настраивать. Если же у сервиса нет собственного клиента для Android, тоже ничего страшного — для работы с VPN-соединением в Android имеется встроенный VPN-клиент, настройка которого осуществляется в следующем порядке:

1. Откройте настройки телефона.
2. Перейдите в меню **Беспроводные сети** | **Еще** (или **Дополнительно**) | **VPN**.
3. Выберите команду **Добавить VPN профиль**, а затем **Добавить PPTP VPN**.
4. Придумайте и введите название VPN-соединения (произвольное), адрес VPN-сервера, имя пользователя, пароль (эти данные вы получите у VPN-провайдера).
5. Вернитесь в меню **Беспроводные сети** | **Еще** (или **Дополнительно**) | **VPN**, выберите для использования созданное VPN-подключение. После успешного подключения все данные станут передаваться в зашифрованном виде.

6.1.4. Сторонние VPN-клиенты

Как уже отмечалось, некоторые VPN-сервисы предоставляют собственные VPN-клиенты. В этом случае лучше воспользоваться такими клиентами, а не встроенным клиентом Android.

Кроме стандартного клиента вы также можете использовать клиент VpnRoot, скачать который можно по ссылке:

https://play.google.com/store/apps/details?id=com.did.vpnroot

Этот клиент не бесплатный, но зато, в отличие от стандартного VPN-клиента, он умеет переподключаться при разрыве соединения.

Можно также порекомендовать и программу DroidVPN, скачать которую можно по ссылке:

https://play.google.com/store/apps/details?id=com.aed.droidvpn

После регистрации на сайте программы вам дадут 100 Мбайт VPN-трафика в день (но подключаться можно будет только к бесплатным серверам), а за дополнительный трафик или за возможность подключения к коммерческим VPN-сервисам придется, хоть и немного, но заплатить.

6.2. Проект Tor в Android

6.2.1. Что такое Tor?

Многим пользователям настольных систем, которые хоть один раз интересовались безопасностью и анонимностью передачи данных в Интернете, знаком проект Tor. Для тех, кто не знает, что такое Tor, — небольшое введение.

Представим, что нам нужно скрыть свой IP-адрес от удаленного узла и полностью «замаскироваться» — чтобы администратор вашей сети или кто-то еще не смог бы определить, какие узлы мы посещаем, и чтобы никто не смог «подслушать» передаваемые нами данные.

Именно для решения таких задач и была создана *распределенная сеть Tor*. Tor (аббревиатура от The Onion Router, дословно «луковый маршрутизатор» — так здесь обыграна как бы многослойная защита, предоставляемая этой сетью) — это свободное (т. е. свободно распространяющееся и абсолютно бесплатное) программное обеспечение, служащее для анонимизации трафика.

> ***«Черному ходу» — нет!***
>
> Поскольку исходный код Tor открыт всем желающим, любой пользователь может проконтролировать Tor на наличие/отсутствие «черного хода», специально созданного для спецслужб или еще кого-то. На данный момент Tor ничем не скомпрометировал себя — его репутация незапятнанна.

Сеть Tor обеспечивает надежную анонимизацию и защищает пользователя от слежки как за посетителями конкретного сайта, так и за всей активностью самого пользователя. К тому же все передаваемые пользователем данные шифруются, что исключает их прослушивание.

Вкратце принцип работы Tor заключается в следующем — при обмене данными между узлом А (ваш компьютер) и узлом Б (удаленный сайт) эти данные передаются в зашифрованном виде через цепочку промежуточных узлов сети. Отсюда следует еще одно преимущество использования Tor, которое наверняка оценят пользователи корпоративных сетей, которым запрещается посещение сайтов, впрямую не связанных с их профессиональной деятельностью. Поскольку узел (нод, от англ. *node*) А обращается к узлу Б не напрямую, а через промежуточные узлы, то это позволяет обойти «черный список» брандмауэра корпоративной сети.

Рассмотрим конкретный пример. Предположим, у вас в офисе «злой» администратор заблокировал доступ сотрудников к социальной сети, к тем же «Одноклассникам» (наверное, это самая популярная сеть на наших просторах, хотя есть и не менее популярные: «ВКонтакте», «Мой мир», Facebook и др.). Сайт **www.odnoklassniki.ru** и будем считать узлом Б, а ваш смартфон назовем узлом А.

Подключение через сеть мобильного оператора?

Вообще-то к «Одноклассникам», находясь на работе, можно подключиться и через сеть мобильного оператора — локальный администратор на нее никак повлиять не может. Однако, согласитесь, обидно, что в зоне действия бесплатной сети Wi-Fi для посещения любимых сайтов придется расходовать платный мобильный трафик.

Итак, вы запускаете программу Tor (далее будет объяснено, откуда ее взять и как точно она называется) и вводите адрес узла Б. Передаваемые вами данные (в данном случае — адрес узла) будут зашифрованы и переданы первому узлу в цепочке — назовем его узел В. Узел В дополнительно шифрует данные и передает узлу Г и т. д. Процесс шифровки и передачи данных будет продолжаться, пока данные не получит последний узел цепочки (скажем, узел Т), который и передаст ваш запрос конечному узлу — Б. Понятно, что на последнем участке (от узла Т к узлу Б) данные уже не будут зашифрованы, поскольку узел Б не поддерживает открытые ключи сети Tor (если бы это было так, то весь Интернет был бы анонимным). Следовательно, ответ конечного узла Б исходному узлу А (запрошенные данные) пройдет по этой цепочке обратно соответственно последовательно дешифруясь на каждом шаге.

Посмотрите на рис. 6.1 — на нем изображен процесс передачи данных между вашим и удаленным компьютерами через сеть Tor. Проанализировав его можно сделать следующие выводы:

- администратор вашей сети (или администратор провайдера) не сможет узнать, какие данные вы передаете, поскольку данные передаются в зашифрованном виде;
- администратор вашей сети не сможет узнать, какой узел вы посещаете, поскольку вместо интересующего вас узла (**www.odnoklassniki.ru**, **www.vkontakte.ru** и т. п.) ваш узел формально обращается к одному из узлов сети Tor — ничем не примечательному узлу с непонятным доменным именем. Тем более, что при каждом новом подключении к Tor первый узел цепочки окажется другим;
- если администратор сети на брандмауэре заблокировал доступ к интересующему вас узлу (**www.odnoklassniki.ru**, **www.vkontakte.ru** и т. п.), то вы сможете обойти это ограничение, поскольку фактически ваш компьютер подключается к совершенно другому узлу (к первому узлу цепочки Tor). Запрещать доступ к этому узлу нет смысла, поскольку при следующем подключении к Tor или при принудительной смене цепочки узел входа в Tor будет уже другим;
- удаленный узел «увидит» только IP-адрес последнего узла цепочки, ваш же IP-адрес будет от него скрыт;
- теоретически перехват данных возможен на последнем участке пути — от последнего узла цепочки Tor (узел Т) до удаленного узла (узел Б). Но для этого потребуется отследить всю цепочку Tor, что технически сделать очень сложно, поскольку она может состоять из десятков узлов. Если же получить доступ к удаленному узлу Б, то все равно нельзя будет понять, кто есть кто, поскольку для этого требуется знать как минимум точку входа в сети Tor и точку выхода из нее.

При подключении к сети Tor для вашего смартфона (компьютера) определяется точка входа (выбирается случайный узел из сотен тысяч узлов Tor), «тоннель» и

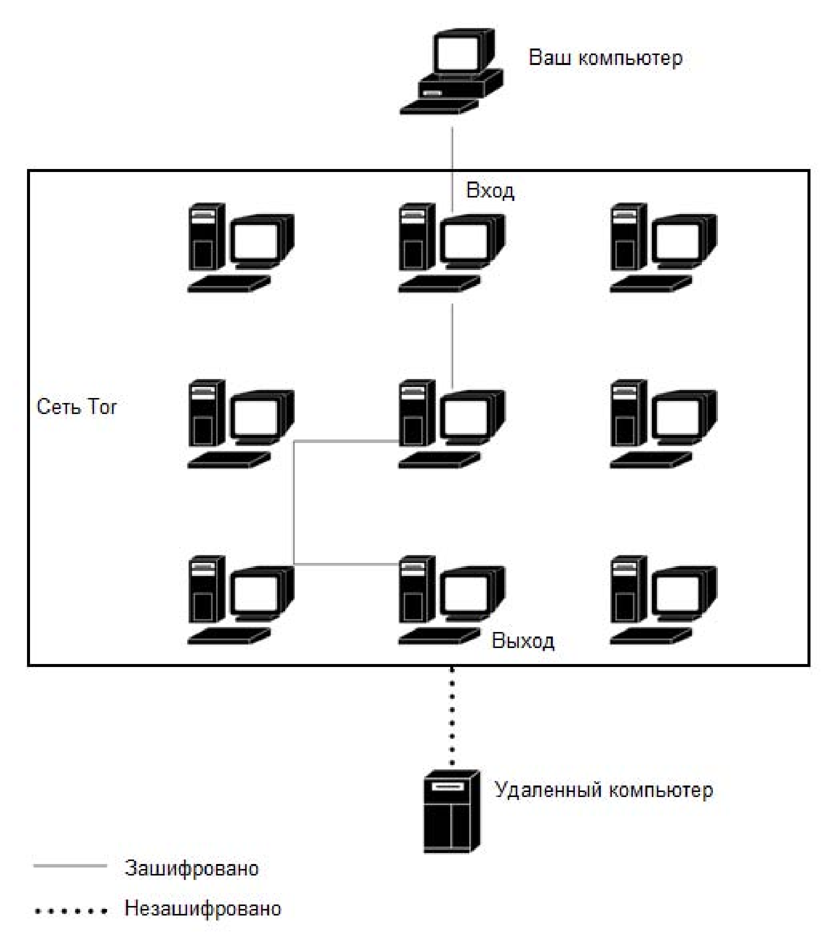


Рис. 6.1. Передача данных через распределенную сеть Tor

точка выхода — т. е. строится цепочка. В процессе работы с сетью иногда возникает необходимость сменить цепочку — это можно сделать без перезагрузки программного обеспечения (позже будет показано, как), что делает работу с сетью максимально комфортной.

Смена цепочки может понадобиться в двух случаях:

- когда нужно сменить конечный IP-адрес (например, чтобы получить IP-адрес, относящийся к определенной стране или городу);
- когда полученная цепочка оказалась слишком медленной. Скорость передачи информации зависит от каналов передачи данных от одного узла цепочки к другому, поэтому сгенерированная цепочка может оказаться нерасторопной. Вы же можете создать другую цепочку — вдруг она окажется быстрее?

Проект Tor кроссплатформенный. Это означает, что клиенты для подключения к Tor есть как для Windows, так и для Linux и Mac OS. Скачать программное обеспечение для настольных систем абсолютно бесплатно можно по адресу:

https://www.torproject.org/

Еще раз хочется отметить, что пользование сетью Tor полностью бесплатно — не нужно никому платить ни за передаваемый трафик, ни за программное обеспечение. В этом ее главное и принципиальное отличие от VPN-сервисов. Но есть и еще одно не менее важное отличие — при каждом подключении к Tor выбирается другая цепочка: другой узел входа и другой узел выхода. При использовании VPN-сервисов сервер у вас будет один, максимум — несколько штук. Соответственно при желании вас можно полностью идентифицировать и выяснить, кому и какие данные вы передаете (конечно, если дело дойдет до международного скандала). В случае с Tor такая задача существенно усложняется, поскольку цепочку передачи данных можно менять совершенно свободно — хоть каждые несколько минут.

6.2.2. Установка Tor в Android

Tor-клиент для Android называется Orbot и загрузить его можно по ссылке:

https://play.google.com/store/apps/details?id=org.torproject.android

Однако установка Orbot не означает, что теперь ваше устройство защищено, и вы можете безопасно передавать данные. Отнюдь. Требуется дополнительная настройка. Внимательно и неспешно выполните следующие действия (желательно сначала прочитать, а потом уже делать):

1. Запустите Orbot и выберите русский язык (рис. 6.2).
2. Дважды нажмите кнопку **Вперед** — этим вы пропустите две информационные страницы.
3. Далее приложение Orbot попытается запросить доступ root. Доступ root нужен для расширенных функций программы, а именно — для прозрачной проксификации. Прозрачная проксификация позволяет защитить все сетевые приложения на вашем устройстве, даже те, которые не предназначены для работы с Tor. Если включить прозрачную проксификацию, тогда все установленные браузеры и другие сетевые программы (Skype, Viber, Twitter и т. п.) станут работать через Tor. Следовательно, ваш трафик будет защищен и анонимизирован. Если же прозрачная проксификация не используется, тогда, чтобы трафик был защищен, потребуется использовать специальные программы, которые предназначены для работы с Orbot. Поскольку процедура получения прав root может быть крайне болезненной для вашего смартфона, установите флажок **Я понимаю и хочу продолжить без прав суперпользователя** (рис. 6.3). Нажмите кнопку **Вперед**.
4. Далее программа подскажет, какие программы нужно установить, чтобы трафик был защищен (рис. 6.4). Понадобится как минимум браузер ORWEB — это обычный браузер, но настроенный для работы с Orbot. Не следует нажимать кнопку для установки ORWEB в приложении Orbot — вы получите сообщение, что такого приложения не существует (небольшой недочет разработчиков Orbot). Лучше найдите и установите ORWEB из Play Маркет отдельно. Так что пока ORWEB не запускайте, а вернитесь в Orbot и нажмите кнопку **Вперед**.

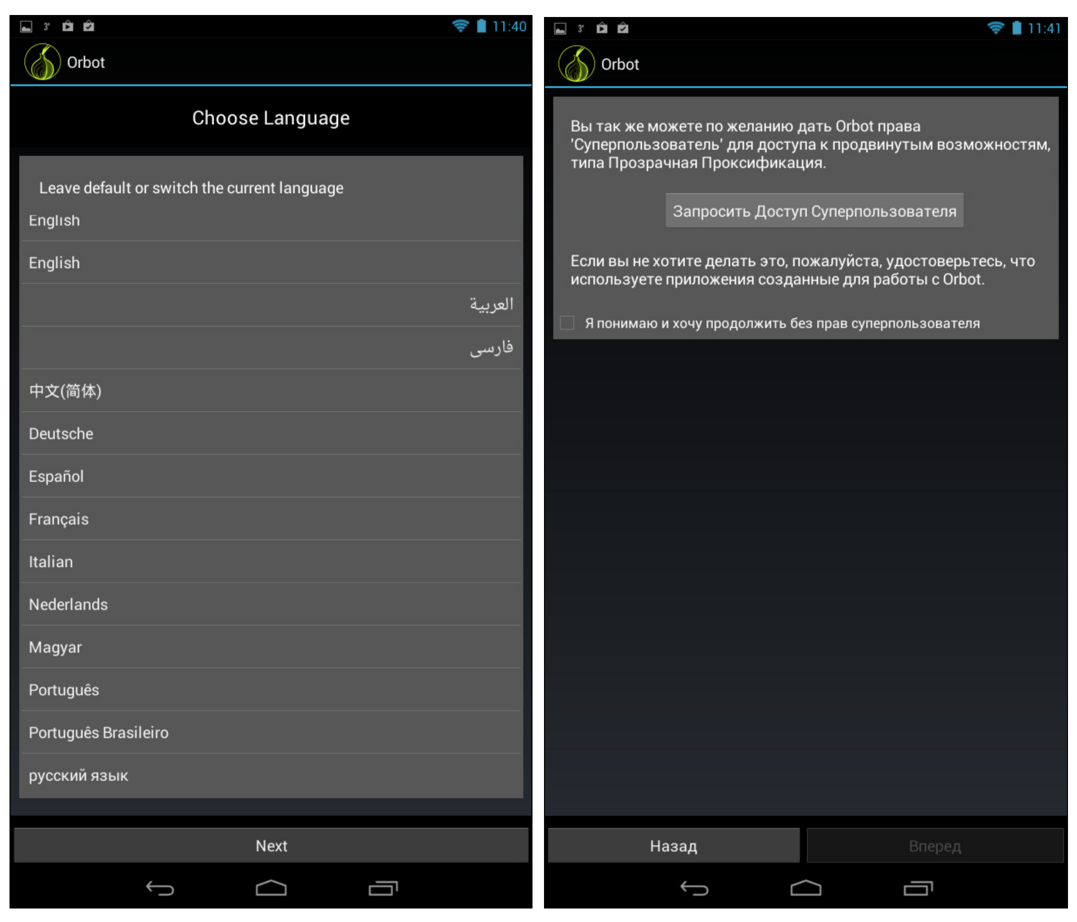


Рис. 6.2. Первый запуск Orbot

Рис. 6.3. Запрос на получение прав суперпользователя

5. Появится еще одно информационное сообщение, нажмите в нем кнопку **Завершить.**
6. Далее вы увидите луковицу (рис. 6.5) — это символ Tor, под ней находится кнопка включения Tor. Нажмите и удерживайте эту кнопку, пока она не поменяет цвет на желтый. Начнется процесс подключения к Tor. Подключение занимает немного времени (несколько десятков секунд), так что придется подождать.
7. После запуска Tor вы получите соответствующее сообщение, а луковица поменяет цвет на зеленый (рис. 6.6).
8. Запустите приложение ORWEB — оно сообщит вам ваш IP-адрес (рис. 6.7), который увидят удаленные узлы, когда вы будете работать через ORWEB.
9. Запустите теперь обычный браузер (например, Chrome) и перейдите по адресу **www.geoiptool.com** — вы получите свой реальный IP-адрес. Если адреса отли-

чаются, значит, все работает, и можно безопасно и анонимно пользоваться браузером ORWEB.

Работаем без прозрачной проксификации

Напомню, поскольку прозрачной проксификации нет, трафик будет защищен только в браузере ORWEB.

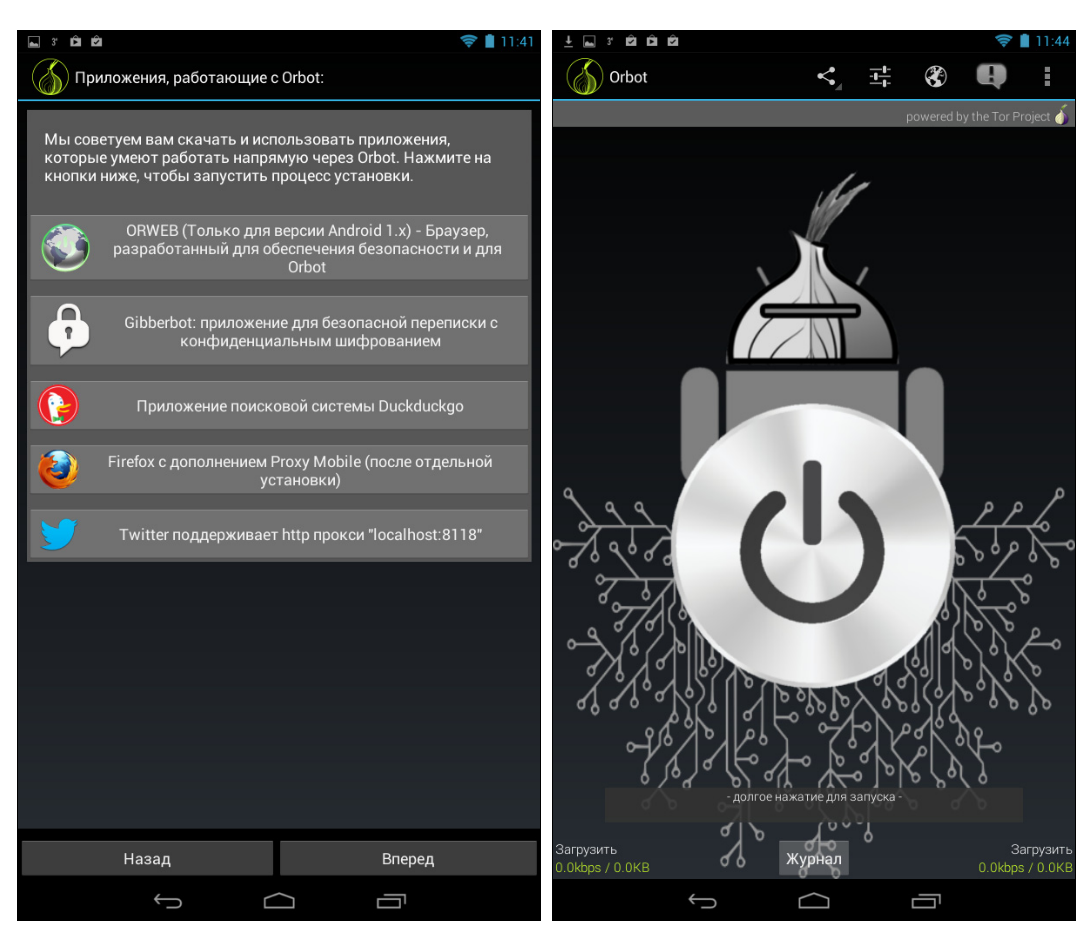


Рис. 6.4. Программы, поддерживающие Orbot

Рис. 6.5. Нажмите и удерживайте кнопку включения

В дальнейшем работать через Orbot нужно так:

1. Сначала запускаем Orbot, нажимаем кнопку включения и ждем, пока Orbot подключится к сети Tor.
2. После подключения к Tor можно запустить и использовать браузер ORWEB.

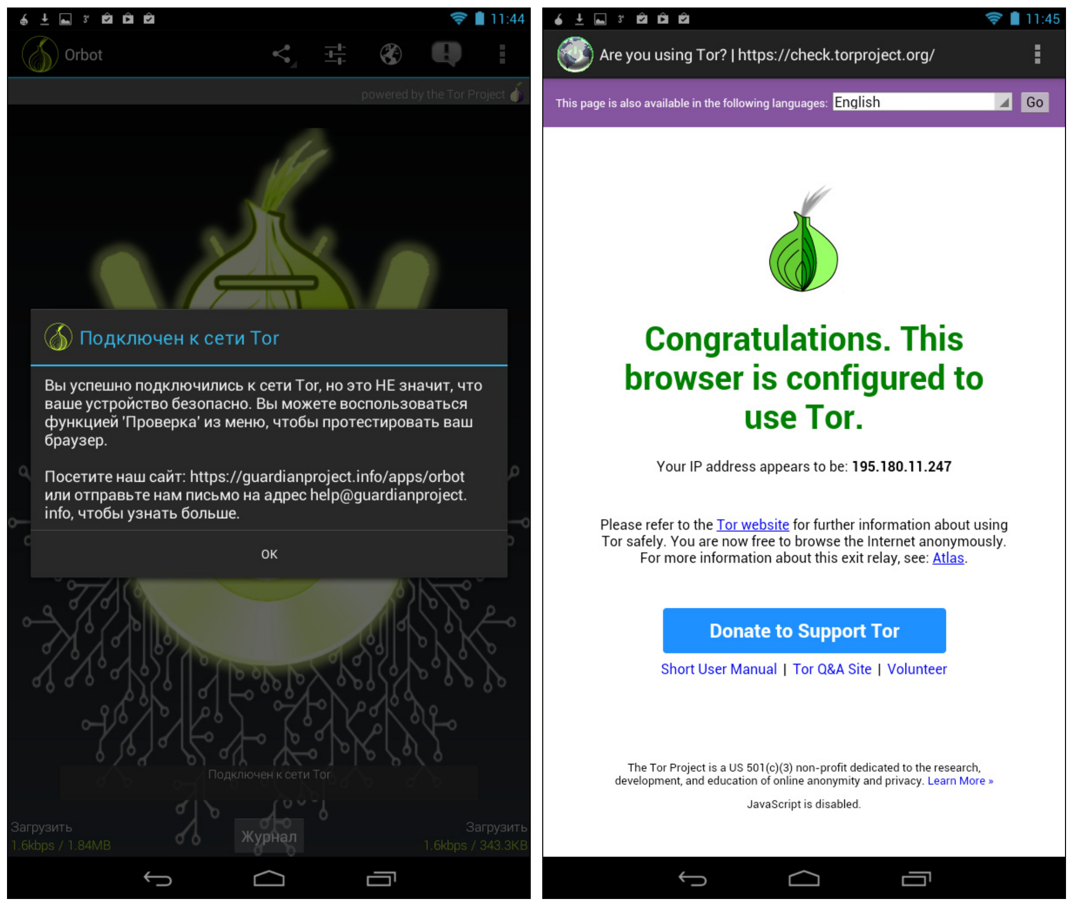


Рис. 6.6. Orbot готов к работе

Рис. 6.7. Браузер ORWEB запущен

6.2.3. Как «подружить» с Tor другие программы?

Чтобы с Tor заработала какая-то сетевая программа (отличная от ORWEB), нужно ее соответствующим образом настроить. Проблема здесь в том, что далеко не все программы позволяют задавать необходимые параметры. Если в настройках программы предусмотрена возможность указать параметры прокси-сервера, тогда ее можно «подружить» с Tor. Просмотрите параметры программы. Если она позволяет прописать прокси-сервер, то укажите IP-адрес прокси 127.0.0.1 и порт 8118.

На некоторых устройствах можно указать общесистемный прокси (это вообще идеальный вариант) так: **Настройки | Беспроводные сети | Настройки WiFi | [Menu] | Дополнительно | Прокси-сервер WiFi**. Однако такая возможность присутствует далеко не на каждом устройстве. А на некоторых прокси работает только через 3G, но не через Wi-Fi.

Если вы принципиально предпочитаете использовать браузер Firefox, а не ORWEB, тогда установите мобильный Firefox и расширение Mobile Private Browsing, чтобы

настроить Firefox на работу через прокси-сервер. Подробные инструкции по установке и настройке этого расширения приведены по адресу:

https://guardianproject.info/apps/firefoxprivacy/

На этой же странице имеются и ссылки для загрузки самого расширения.

Можно также для работы с Tor использовать и браузер Opera Mobile Classic, настройка которого будет описана в конце этой главы. Opera Mobile Classic — один из немногих браузеров для Android, позволяющий задать адреса прокси-серверов.

В Play Маркет можно найти программы, позволяющие задать общесистемный прокси (вроде ProxyDroid), но все эти программы требуют права root, а если вы уж решитесь на их получение (см. об этом *главу 10*), то проще включить прозрачную проксификацию Tor, и не использовать какие-либо другие программы.

6.2.4. Задание выходных узлов

Одной из задач, которые ставятся перед Tor, является получение IP-адреса определенной страны. Бывает так, что та или иная страна какой-то свой ресурс может закрыть для доступа иностранным пользователям или пользователям определенной страны. Чтобы преодолеть такие ограничения, можно использовать Tor, предварительно настроив его на использование определенных выходных узлов.

> ***«Иностранцы» в своей стране***
>
> Ситуация не надумана. Когда-то компания «Укртелеком» раздавала своим пользователям IP-адреса, принадлежащие какой-то европейской стране (кажется, Нидерландам, но точно уже не помню). В результате пользователи не могли получить доступ к ресурсам, которые разрешали доступ только узлам, находящимся в пределах точки обмена трафика UA-IX. Так множество пользователей «Укртелекома» стали «иностранцами» в своей же стране, никуда не выезжая за ее пределы.

Выходной узел — это последний узел в цепочке Tor, именно его адрес увидит удаленный узел, к которому вы обращаетесь. Задать выходной узел можно в настройках Orbot:

1. Откройте страницу настроек Orbot (рис. 6.8).
2. Задайте выходные узлы. Например, для получения IP-адреса из США нужно записать код страны в фигурных скобках: {US} (рис. 6.9).
3. Нажмите кнопку **OK**.
4. Остановите Orbot и запустите его заново.

В фигурных скобках указывается так называемый *ISO-код* страны. Список кодов вы без проблем найдете в Интернете. Привожу здесь лишь некоторые коды:

- BR — Бразилия;
- CA — Канада;
- CN — Китай;
- DE — Германия;
- GB — Великобритания;
- RU — Россия;
- UA — Украина;
- US — США.

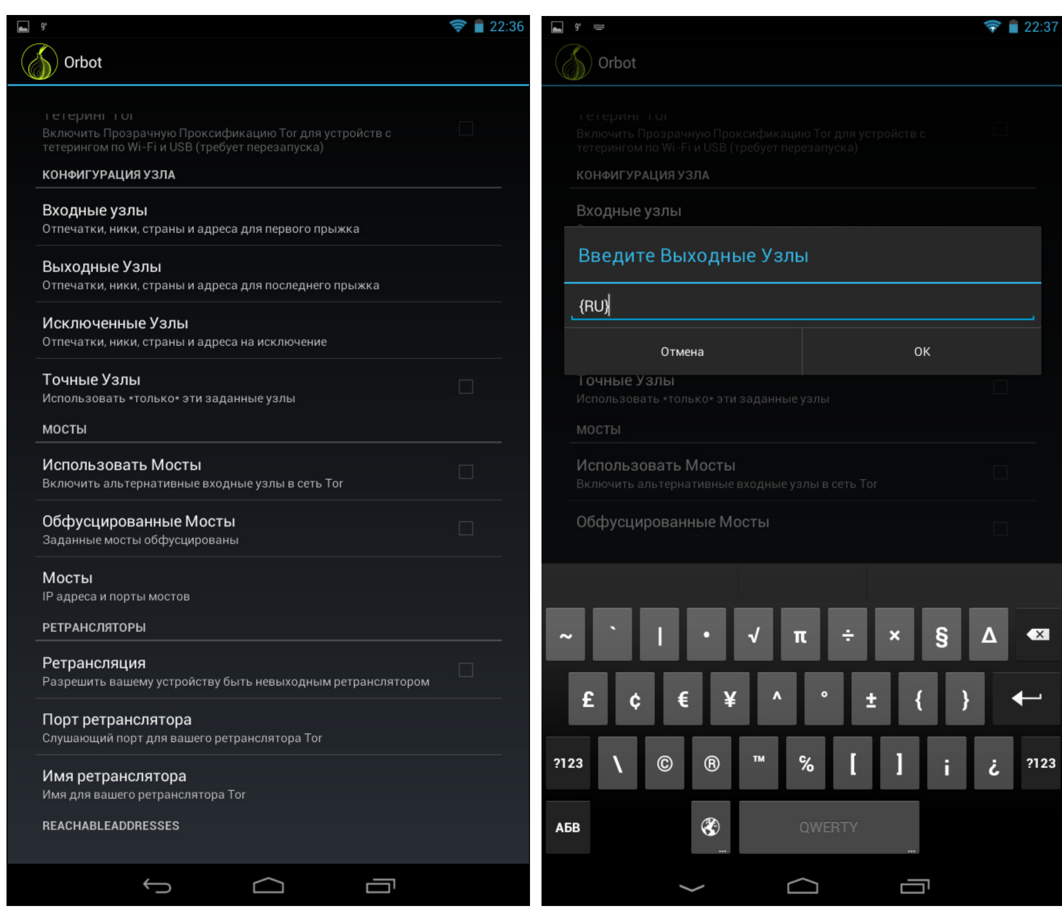


Рис. 6.8. Страница настроек Orbot

Рис. 6.9. Задаем выходные узлы

География Tor очень впечатляет — практически в каждой стране есть ее выходные узлы. Так что Tor — весьма удачный проект и удовлетворит запросы безопасности и анонимизации трафика большинства пользователей.

6.2.5. Что лучше: VPN или Tor?

В этой главе было рассмотрено два альтернативных подхода к шифрованию передаваемого по сети трафика: VPN-сервисы и Tor. Какой способ выбрать?

Ничего не остается, как провести их сравнение.

Преимущества VPN:

- *удобство использования*. Некоторые VPN-сервисы предоставляют собственные VPN-клиенты, которые практически не требуется настраивать. Нужно только запустить их и наслаждаться зашифрованной передачей данных;
- *весь трафик, генерируемый вашим устройством, шифруется*. При этом вам не нужны права root. В случае же с Tor для запуска прозрачной проксификации по-

требуются права root. В противном случае шифроваться станет трафик только тех приложений, которые поддерживают браузер Orbot, трафик остальных приложений шифроваться не будет;

- *высокая скорость доступа*. Скорость доступа к Интернету через VPN-сервис хоть и окажется немного ниже, чем скорость обычного доступа в Интернет, но все же останется на довольно высоком уровне.

На этом преимущества VPN-сервисов заканчиваются и начинаются недостатки:

- не всегда у VPN-сервисов имеются собственные VPN-клиенты, и не все клиенты поддерживают все распространенные протоколы. Хорошо, хоть все VPN-сервисы обеспечивают работу по протоколу PPTP, который поддерживает встроенный VPN-клиент Android;
- доступ к VPN-серверам платный, и не все предоставляют тестовый доступ: утром — деньги, вечером — стулья;
- в большинстве случаев выбор точек присутствия ограничен. Как правило, можно выбрать сервер из США, Канады и нескольких европейских стран;
- вся ваша активность протоколируется и хранится на серверах VPN-сервиса несколько лет. Выводы делайте сами. По сути, это и есть самый значительный недостаток коммерческих VPN-сервисов;
- российские и украинские VPN-серверы из соображений конфиденциальности данных использовать вообще нельзя — при малейшем подозрении вся информация о вас будет передана, куда следует. Поэтому в этой главе рассматриваются только зарубежные серверы. Они хоть и тоже не образец конфиденциальности, но даже если кто-то сильно захочет узнать, что вы делали в Интернете и кому что передавали, международная бюрократия даст вам огромную фору во времени.

Теперь рассмотрим преимущества Tor:

- самое главное преимущество сети Tor — что это свободный проект, узлами сети Tor выступают машины энтузиастов, и *никакая информация о вашей активности не записывается*. К тому же каждый следующий узел в цепочке Tor не знает о вас ничего, кроме того, что данные пришли с предыдущего узла. Проследить цепочки Tor очень сложно с технической точки зрения;
- при включенной прозрачной проксификации *через Tor могут работать любые сетевые приложения*;
- *сеть Tor абсолютно бесплатная* — вы реально ни за что не платите;
- *огромный выбор точек присутствия* — в каждой стране есть узлы Tor, и вы можете выбрать выходной узел с любым нужным вам IP-адресом.

Недостатки у Tor тоже есть:

- не очень высокая скорость доступа. Впрочем, с каждым годом ситуация становится лучше, т. к. увеличивается пропускная способность каждого Tor-узла. Скажем, в 2005 году скорость в 1 Мбит/с мне казалась фантастической, а уже в 2009-м скорость 50 Мбит/с стала нормой для многих;

- чтобы заработала прозрачная проксификация, нужны права root, а их получение не всегда оправданно. Без прав root с сервисом Orbot (через Tor) будут работать только определенные приложения, «заточенные» под Tor, а таковых совсем мало. Однако если вам нужен только интернет-браузер, то установкой браузера ORWEB эта проблема практически снимается.

Учитывая все сказанное, оптимальный выбор — Tor, даже несмотря на некоторые проблемы с прозрачной проксификацией. Окончательное слово, конечно же, за вами.

6.3. Сеть I2P

6.3.1. Что такое I2P?

В предыдущем разделе мы познакомились с распределенной сетью Tor, позволяющей зашифровать и анонимизировать трафик. Здесь будет рассмотрен другой проект анонимизации — I2P (Invisible Internet Project, проект «Невидимый Интернет»). I2P — это так называемая *оверлейная* сеть, т. е. сеть, работающая «поверх» обычного Интернета. Получается, что I2P — как бы Интернет в Интернете.

В соответствии со своей структурой сеть I2P обеспечивает функционирование внутри себя многих сетевых служб: сайтов (технология eepsite), почты, систем мгновенного обмена сообщениями и даже торрент-трекеров (BitTorrent, EDonkey, Kad, Gnutella и др.). А для последних I2P — просто рай, до сих пор не понимаю, почему все торрент-трекеры не перекочевали еще в I2P. Скорее всего, потому, что многие пользователи не знают об I2P и не понимают, как в ней работать. Вот сейчас этот пробел в ваших знаниях мы и восполним, а уж использовать I2P или нет — решайте сами.

Преимущества I2P

Итак, чем же I2P полезна обычным пользователям? Начнем с торрент-трекеров. Загружая фильм (программу, музыкальную композицию и т. п.) с торрент-трекера (не говоря уже о раздаче этого контента), вы нарушаете законодательство об авторских правах. А во время загрузки (раздачи) контента через торрент-трекер ваш IP-адрес виден всем. Теоретически, при самом неблагоприятном для вас раскладе правоохранительные органы могут нанести вам весьма неприятный визит.

Однако при работе в I2P такого не произойдет никогда, поскольку ваш IP-адрес будет зашифрован, а маршрутизация осуществляется по так называемым *туннелям*. Другими словами, доказать, что это именно вы скачали там-то и там-то фильм, — практически нереально. Конечно, нельзя утверждать, что невозможно вовсе. При особом желании доказать можно, но для этого придется потратить столько времени, средств и других ресурсов, что окажется проще снять другой фильм, чем доказывать, что вы скачали с трекера именно этот (а, сами понимаете, вы не один такой пользователь).

В сети I2P любой желающий может создать собственный сайт, причем абсолютно бесплатно, — не придется платить ни за регистрацию имени, ни за доменное имя

вида **name.i2p**. А хостинг можно развернуть на своем компьютере, установив связку Apache + PHP + MySQL (если вы не понимаете, как это сделать, достаточно установить XAMPP[1] — благодаря этому продукту данная связка устанавливается очень легко). Сайты внутри I2P-сети скрытые — т. е., чтобы выяснить, на каком именно компьютере «лежит» тот или иной сайт, нужно опять-таки потратить массу ресурсов.

Скрытый сайт можно создать и в сети Tor, однако там вместо удобного имени вида **name.i2p** будет сгенерирован длиннющий хэш, который вам придется хранить в отдельном текстовом файле, — запомнить вы его не сможете.

Кроме скрытых сайтов и анонимных торрентов, в I2P работает анонимная почта, можно также организовать анонимное общение через популярные клиенты мгновенного обмена сообщениями и даже настроить Skype для работы через I2P. Как известно, Skype использует проприетарные и очень сложные алгоритмы шифрования. Поддерживают они прослушку или нет — известно одним разработчикам Skype (в последнее время появляется все больше слухов, что прослушка разговоров в Skype возможна). Когда же вы отправляете Skype-трафик через I2P (или через Tor, как было показано ранее), прежде, чем добраться до разговора в Skype, желающим прослушать ваши разговоры придется вскрыть несколько слоев шифрования в I2P. Таким образом, использование I2P (или Tor) значительно усложняет задачу прослушки.

Еще два бонуса, предоставляемых сетью I2P обычным пользователям, заключаются в поддержке русского языка, а также кроссплатформенности — поскольку для создания программного обеспечения I2P использовался язык Java, то ПО для I2P можно запускать как в Windows, так и в Linux, Mac OS, Solaris и прочих операционных системах.

Недостатки I2P

А теперь ложка дегтя. Нет ничего идеального, и I2P — тоже не идеальна. Начнем с самой концепции I2P. Анонимизация и шифрование трафика происходит лишь внутри этой сети. Работая с I2P, вы можете обратиться только к I2P-ресурсам (к I2P-сайтам, почте, трекерам и т. д.). Если вы обращаетесь к ресурсу, не принадлежащему к I2P, защита не обеспечивается. С той же Tor все намного удобнее, поскольку вы можете обращаться к любым ресурсам Интернета, и при этом трафик будет анонимизирован и защищен.

Это и есть основной недостаток I2P. Но существуют еще два отрицательных момента, о которых вы также должны знать. Прежде всего — в I2P-сети очень мало русскоязычных ресурсов. Больше она популярна в Германии — немецких ресурсов и англоязычных сайтов в I2P очень много, а вот русскоязычных — единицы. Будет ли вам интересна I2P, зависит от вашего владения английским и немецким языками и, разумеется, от информации, которую вы хотите найти в I2P.

---

[1] XAMPP — кроссплатформенная сборка веб-сервера, содержащая Apache, MySQL, интерпретатор скриптов PHP, язык программирования Perl и большое количество дополнительных библиотек, позволяющих запустить полноценный веб-сервер.

Еще один недостаток — это существенные потоки трафика, проходящие через ваш компьютер. Если в Tor вы могли работать только в качестве клиента, то в сети I2P через ваш компьютер передается трафик других I2P-пользователей. Трафик зашифрован, тут особо беспокоиться не о чем, но если ваш интернет-тариф учитывает объем трафика, то I2P вам вряд ли подойдет, поскольку вы будете вынуждены платить и за свой трафик, и за трафик других пользователей, проходящий через ваш компьютер. Вы можете зайти в I2P, часик посидеть почитать какие-либо сайты, а за это время через ваш компьютер будет пропущено несколько гигабайтов трафика.

6.3.2. Шифрование информации в I2P

Весь трафик в сети I2P, в отличие от Tor, шифруется от отправителя к получателю. В общей сложности используются четыре уровня шифрования (сквозное, чесночное, туннельное и шифрование транспортного уровня). Перед шифрованием I2P добавляет в отправляемый пакет случайное количество произвольных байтов, чтобы еще больше затруднить попытки анализа содержимого пакета и его блокировки.

В качестве адресов сети применяются криптографические идентификаторы (открытые криптографические ключи), не имеющие никакой логической связи с реальным компьютером. В сети I2P нигде не используются IP-адреса, поэтому определить настоящий IP-адрес узла и, следовательно, установить его местонахождение невозможно.

Каждое сетевое приложение, работающее через I2P, строит для себя анонимные зашифрованные туннели — обычно одностороннего типа, когда исходящий трафик идет через одни туннели, а входящий — через другие. Выяснить, какое приложение создало тот или иной туннель, — тоже невозможно (точнее, очень сложно, поэтому будем считать, что это практически невозможно).

Все пакеты, передаваемые по сети, могут расходиться по разным туннелям, что делает бессмысленной попытку перехвата (прослушки) данных. И в самом деле — поскольку данные передаются по разным туннелям, проанализировать поток данных даже с помощью сниффера[1] не получится. Каждые 10 минут происходит смена уже созданных туннелей на новые с новыми цифровыми подписями и ключами шифрования (у каждого туннеля свой ключ шифрования и своя цифровая подпись).

Вам не нужно беспокоиться, чтобы прикладные программы обеспечивали шифрование трафика. Если существует недоверие к программам, имеющим закрытый исходный код (взять тот же Skype), можно или попытаться заставить эти программы работать через I2P, или поискать альтернативные программы с открытым кодом. Так, вместо Skype можно использовать Ekiga — простую программу для IP-телефонии. Правда, она не умеет шифровать данные (они передаются в открытом виде), но о шифровании позаботится I2P. Конечно, ваш собеседник тоже должен исполь-

[1] Сниффер — анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа либо только анализа сетевого трафика.

зовать I2P, иначе толку от всех этих мероприятий (настройки Skype для работы через I2P или установки и использования Ekiga) не будет.

Шифрование и дешифрование пакетов осуществляются соответственно на стороне отправителя (шифрование) и на стороне получателя (расшифровка). В отличие от Tor, никто из промежуточных участников обмена не может перехватить зашифрованные данные и никто из участников не знает, кто на самом деле является отправителем, а кто получателем, поскольку передающий пакеты узел может быть как отправителем, так и промежуточным узлом.

Промежуточный узел не может узнать конечные точки (кто отправил пакеты и куда они следуют), так же он не может определить, что случилось с только что переданным следующему узлу пакетом: принял он его себе (т. е. следующий узел является получателем) или передал следующему узлу.

В I2P используются следующие методы (алгоритмы) шифрования:

- AES (256 битов);
- схема Эль-Гамаля (2048 битов);
- алгоритм Диффи-Хеллмана (2048 битов);
- DSA (1024 бита);
- HMAC (256 битов);
- SHA256 (256 битов).

6.3.3. Как работать с I2P?

Все очень и очень просто. Принцип работы I2P с точки зрения неискушенного пользователя такой же, как и в случае с Tor. Вы устанавливаете I2P на свой компьютер, изменяете, если сочтете нужным, настройки по умолчанию (хотя в 99 % случаев этого делать не придется, поскольку I2P — это программа, работающая «из коробки», т. е. не требующая настройки) и настраиваете свои сетевые программы — в их настройках следует указать использование прокси-сервера с IP-адресом 127.0.0.1 (порт 4444). Аналогичные действия мы проделывали при настройке сетевых программ на использование прокси-сервера Tor (только номер порта был другим).

После этого вы можете заходить на I2P-сайты сети, например, на **http://i2p2.i2p** — это официальный сайт проекта I2P.

По трафику, отправляемому вашим компьютером в Интернет, очень сложно понять, что от вас исходит — то ли это ваш трафик, то ли это транзитный трафик других клиентов I2P-сети. Другими словами, доказать причастность кого-либо к конкретной сетевой активности весьма тяжело.

6.3.4. Tor или I2P?

Так что же лучше: Tor или I2P? Такой вопрос рано или поздно задаст любой пользователь, поработавший хотя бы раз с Tor или I2P. Спешу вас разочаровать, срав-

нивать I2P и Tor нельзя — это все равно, что сравнивать апельсины с яблоками. Кому-то нравятся апельсины, а кому-то — яблоки. Из яблок не получится апельсиновый сок, и наоборот. Каждая из сетей призвана решать свои задачи, поэтому выбирать между I2P и Tor нужно исходя из поставленных задач.

Сеть I2P — это изолированная, закрытая сеть без выхода во «внешний» Интернет. И пусть в I2P имеется «прокси», позволяющий выйти в Интернет, но это особо не влияет на функционирование сети I2P в целом. I2P не предназначена для обычного серфинга в открытом Интернете. I2P идеальна для анонимного и безопасного обмена файлами, анонимного общения, анонимного хостинга сайтов внутри I2P-сети.

Концепция Tor несколько иная. Изначально Tor разрабатывалась для работы с открытым Интернетом. С его помощью, как было показано ранее, можно легко посещать заблокированные сайты, анонимно посещать обычные сайты и т. п.

Давайте подытожим:

- вам нужно *анонимное общение* (например, по Skype или ICQ)? Тогда лучше воспользоваться I2P. При этом человек, с которым вы собираетесь общаться, тоже должен использовать I2P;
- если же вам нужно *анонимно посетить* тот или иной сайт или же посетить сайт, заблокированный «злым» администратором, тогда следует воспользоваться Tor. Использование Tor можно сравнить с маскировкой, а вот I2P является своеобразным подпольем мировой Сети.

Что же касается преимуществ и недостатков, то они есть у каждой сети, но перечислять мы их не будем, поскольку эти недостатки незначительны, и при использовании той или иной сети по назначению вы о них даже и не вспомните.

6.3.5. Программное обеспечение для Android

Скачать программное обеспечение для работы с I2P в Android можно по ссылке:

http://android-manual.ru/apk/i2p.apk

В Play Маркет вы не найдете этой программы, можете даже не искать. Для установки программы нужно разрешить установку программ из неизвестных источников. Для этого перейдите в меню **Настройки | Безопасность** и *включите* параметр **Неизвестные источники**.

После запуска утилиты подождите примерно полчаса — за это время утилита лучше интегрируется в сеть I2P.

Для работы с утилитой нужен браузер, позволяющий установить прокси. Установите, например, Opera Mobile (именно Mobile, а не просто Opera). Затем в адресной строке браузера введите `opera:config`. Вы увидите параметры **HTTP Server** и **HTTPS Server**. Для обоих параметров установите значение `127.0.0.1:4444` (рис. 6.10).

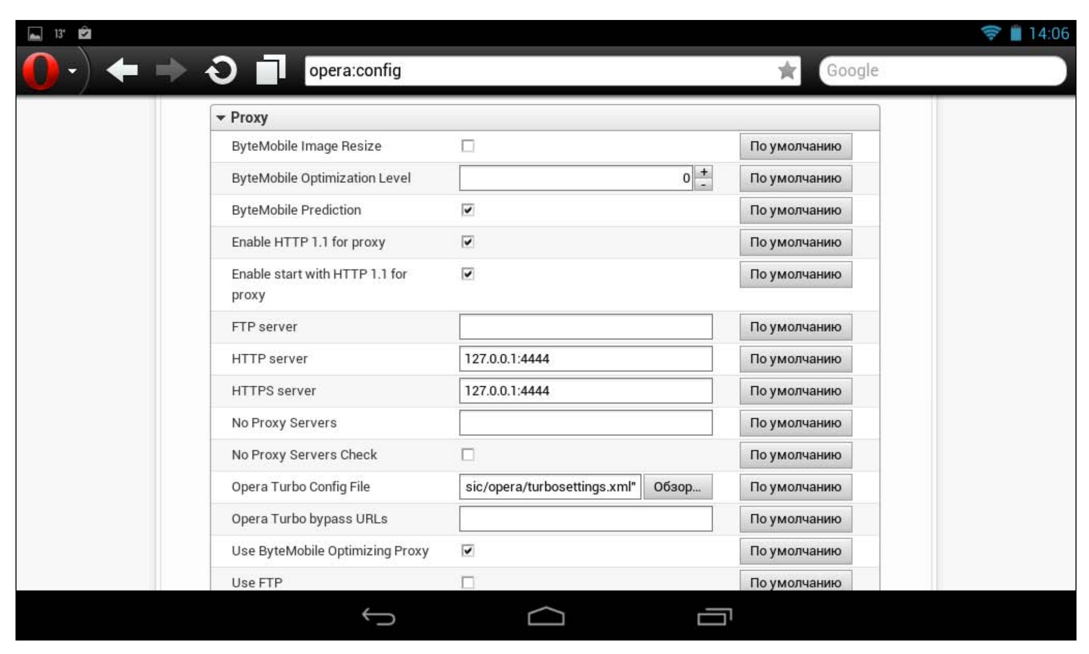


Рис. 6.10. Настройка браузера Opera Mobile Classic

Браузер Opera Mobile Classic

Еще раз отмечу, что нужно использовать браузер Opera Mobile Classic, а не просто Opera. В браузере Opera адрес `opera:config` (редактор настроек) работать не будет. Правильная ссылка на установку браузера из Play Маркет:

https://play.google.com/store/apps/details?id=com.opera.browser.classic

Включите также опции **Use HTTP** и **Use HTTPS**.

Теперь ваш браузер Opera Mobile настроен на использование сети I2P. Учтите, что I2P-сайты загружаются очень медленно, поэтому запаситесь терпением.



ГЛАВА 7

Как найти украденное Android-устройство?

7.1. Постановка задачи

Счастливые обладатели iPhone давно пользуются сервисом поиска потерянного телефона. Более того, украденный iPhone может уничтожить все данные — стереть все контакты, удалить SMS и фотографии. Даже если вернуть устройство не получится, можно хотя бы обезопасить себя лично.

Обладатели iPhone счастливы потому, что весь функционал, описанный в первом абзаце, доступен стандартными средствами, и нужно только научиться их использовать. С Android не все так просто. В Play Маркет вы найдете несчетное множество различных трекеров, позволяющих отследить расположение смартфона/планшета, а также выполнить с ним некоторые дополнительные действия. Лично я перебрал с десяток таких программ (ради интереса, конечно, поскольку решение я знал заранее). Некоторые из них вообще не работают, некоторые точно определяют местоположение устройства, но что делать дальше и каким образом отследить устройство, если вы его потеряли, — непонятно. Такие трекеры лучше использовать для поиска себя, поскольку они умеют хорошо отвечать только на вопрос «где я?». А вот ответа на вопрос «где мой телефон?» они дать не могут.

Компания Google, понаблюдав за всем этим безобразием, выпустила, наконец, и собственное приложение, которое обеспечивает тот же функционал, что и iOS. Теперь пользователи Android более не чувствуют себя обделенными. Приложение Удаленное управление Android позволяет определить местоположение всех ваших Android-устройств, отображает местоположение каждого устройства на карте, а также может уничтожить ваши персональные данные, если телефон все-таки украден, и вернуть его не получилось.

Учитывая, что это приложение — разработка Google, и что сервис абсолютно бесплатен, вы вряд ли найдете лучшее. К тому же удаленное управление можно использовать не только для поиска именно украденного телефона. Вот несколько типичных сценариев:

- *определение местоположения членов семьи*. Речь идет не о банальной слежке, а о безопасности — вы, например, всегда будете знать, где ваши дети. И если ре-

бенок отправился со школой на загородную экскурсию, вам не придется надоедать ему вопросом «ты где?» — можно открыть веб-страницу и посмотреть, где он находится;

- *определение местонахождения автомобиля*. Спутниковая сигнализация стоит дорого, к тому же требует ежемесячной платы. Конечно, есть GPS-сигнализация, но если сигнализация уже установлена, а в ней нет такой функции, то купите самый дешевый Android-телефон и установите на него приложение Удаленное управление. Теперь вы будете знать, где находится ваш автомобиль в случае неприятностей. Конечно, придется решить вопрос с питанием этого самого телефона, но вариантов тут может быть множество, и я уверен, что вы что-нибудь придумаете;
- *определение местонахождения коммерческих автомобилей*. Приложение Удаленное управление может также с успехом использоваться небольшой компанией, которая занимается доставкой чего-нибудь (например, еды) по городу для отслеживания своих автомобилей. Профессиональные GPS-трекеры и специальное программное обеспечение, как уже отмечалось, стоят дорого, а этот сценарий практически не требует вложений. Нужно всего лишь оборудовать каждый автомобиль Android-устройством.

7.2. Использование Удаленного управления Android

Прежде всего приложение Удаленное управление нужно установить. Чтобы вы не перепутали и установили именно то приложение, воспользуйтесь следующей ссылкой:

https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=ru

При первом запуске приложения нужно разрешить Google определять приблизительное местоположение устройства. Для этого просто нажмите кнопку **Разрешить** (рис. 7.1).

Затем следует ввести пароль от вашего Google-аккаунта, и уже через несколько секунд вы увидите ваше местоположение (рис. 7.2).

Теперь нажмите кнопку **Настроить блокировку и очистку** и в открывшейся панели укажите, можно ли будет удаленно заблокировать ваш телефон или вовсе удалить с него все данные. Стоит отметить, что эта функция по умолчанию выключена (рис. 7.3). Если вы не хотите, чтобы злоумышленники использовали ваши личные данные против вас, установите соответствующий флажок.

Итак, вы установили приложение Удаленное управление Android на свой телефон. Что делать дальше? Откройте браузер на своем ноутбуке или любом другом устройстве и введите следующий адрес:

https://www.google.com/android/devicemanager?hl=ru

Войдите под своим аккаунтом Google, и вы сможете отслеживать местоположение всех устройств, связанных с этим аккаунтом (всех устройств, на которые вы установили приложение Удаленное управление Android и на которых используется один и тот же аккаунт Google). Интерфейс управления приведен на рис. 7.4.

Рис. 7.1. Нажмите кнопку **Разрешить**

Рис. 7.2. Определение местоположения устройства

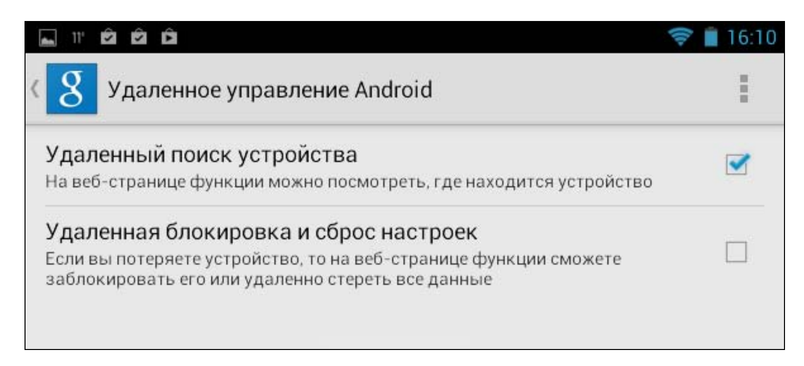


Рис. 7.3. Параметры удаленного управления

Рис. 7.4. Местоположение телефона определено

7.3. Некоторые нюансы

В заключение этой главы нужно кое-что уточнить:

- местоположение определяется примерное, а не точное. Страна и город будут в большинстве случаев определены правильно, а вот с улицей может произойти казус. Поэтому не спешите обвинять ребенка в том, что его не было на уроках! Вполне вероятно, что сервис мог немного ошибиться. Также, учитывая погрешность этого метода, нельзя со стопроцентной уверенностью сказать, находится ли ваш ребенок в школе или отошел от здания на несколько сотен метров. Помните, информация приблизительная;

- местоположение определяется с использованием сети оператора. Другими словами, чтобы все работало, нужен доступ к Интернету, а GPS здесь не задействуется вовсе. А чтобы был доступ к Интернету, следует регулярно пополнять счет мобильного телефона, — полагаю, здесь все понятно;
- некоторые устройства, например планшеты, не оснащены 3G-модулем и к Интернету подключаются только через Wi-Fi, следовательно, если такое устройство окажется за пределами зоны действия сети Wi-Fi, определить его местоположение не получится;
- если телефон действительно украли, напишите заявление в правоохранительные органы, и далее нужно действовать совместно, не следует пытаться отобрать его у похитителя самостоятельно. Мало того, что вы подвергаете свое здоровье, а может, и жизнь опасности, так еще ваши действия могут быть расценены как противозаконные (увы, у нас такие законы);
- если у вас несколько телефонов, настройте на всех телефонах один и тот же аккаунт Google, тогда вы сможете определять местоположение всех устройств сразу на одной интернет-странице.

ГЛАВА 8



Личная безопасность

8.1. Несколько вводных слов

Приложений для Android создано множество, и при желании можно найти приложения для самых разных задач. Существуют и приложения для обеспечения личной безопасности. В этой главе мы рассмотрим два типа таких приложений: приложения с кнопкой SOS, работающие по принципу тревожной кнопки, и приложения для записи телефонных разговоров.

Приложения, работающие по принципу тревожной кнопки, могут сообщить вашим друзьям и родственникам о том, что вы попали в беду. При этом, как правило, на номер телефона, назначенного в качестве тревожного, отправляется соответствующее SMS-сообщение и ваши координаты (ссылка на карту). Как будут развиваться дальнейшие события, зависит от тех, кому пришло такое оповещение, — они могут позвонить в службу спасения, полицию, скорую помощь или же самостоятельно выехать на то место, где вы нажали тревожную кнопку. Другими словами, ваше спасение зависит только от владельцев тревожного телефона, экстренные службы о нажатии вами этой кнопки программы не оповещают.

Что же касается приложений для записи телефонных разговоров, то они могут пригодиться, если вам кто-то угрожает. Полагаю, доказательством в суде такая запись станет вряд ли, но у вас останется хоть какое-то подтверждение своих слов — в любом случае такая «улика» лучше, чем вообще ничего. Как бы там ни было, относительно ее юридической силы вам необходимо проконсультироваться с юристами — я в юридических вопросах не силен, зато помогу с технической частью.

8.2. Мобильный спасатель

Мобильный спасатель — это официальное приложение от МЧС России. Приложение позволяет позвонить в службу спасения, а также оповестить родственников и друзей о том, что с вами произошла экстренная ситуация.

Позвонить в службу спасения можно, конечно, и без этого приложения — достаточно набрать 112, к тому же для звонков на 112 не нужна даже SIM-карта. Но при

нажатии большой красной кнопки **Послать сигнал SOS** (рис. 8.1) приложение автоматически определит регион вашего нахождения, оператора сотовой связи, выберет из базы необходимый номер экстренной службы и осуществит вызов. Одновременно с вызовом службы спасения выбранные вами контакты получат уведомление о том, что вы попали в экстренную ситуацию.

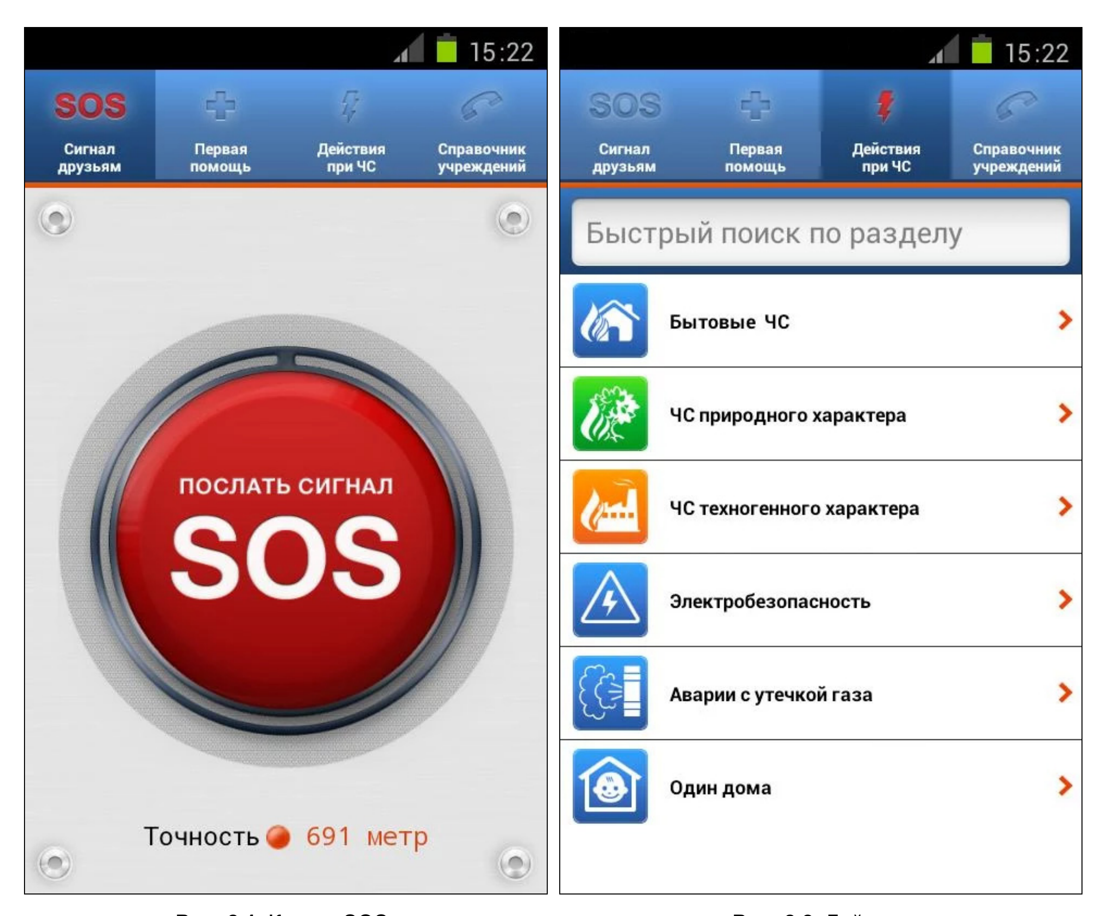


Рис. 8.1. Кнопка SOS

Рис. 8.2. Действия при чрезвычайной ситуации

Но одной только кнопкой SOS функциональность программы не ограничивается. Приложение содержит отличный справочник: как действий во время чрезвычайной ситуации (рис. 8.2), так и адресов ближайших учреждений, где вам в случае необходимости смогут помочь (рис. 8.3).

Приложение неплохое и совершенно бесплатное. Установить его можно по ссылке:

https://play.google.com/store/apps/details?id=ru.sitesoft.mobileRescuer

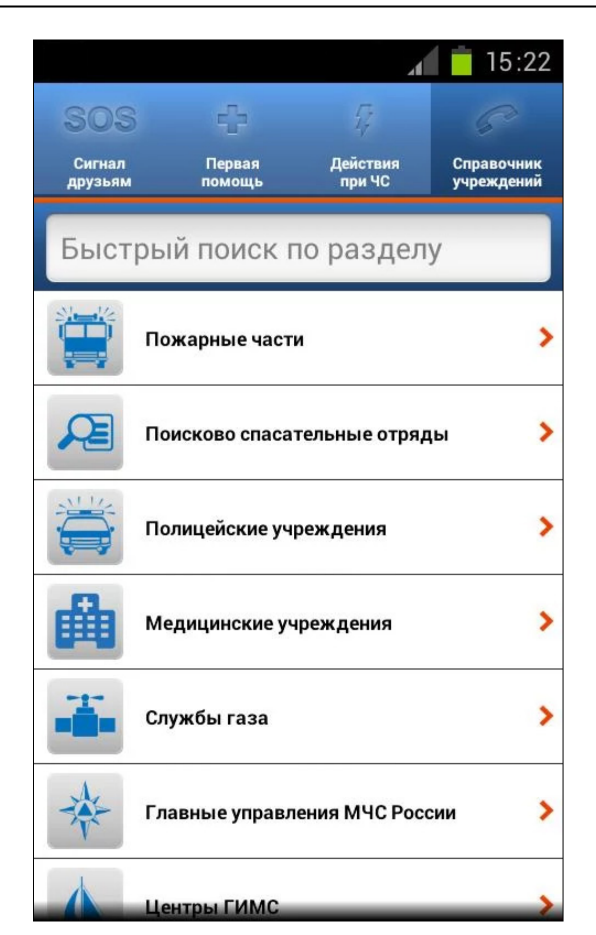


Рис. 8.3. Список учреждений МЧС

8.3. Приложение I'm Getting Arrested

Изначально это приложение замышлялось для уведомления родных и близких о том, что вы арестованы. Как правило, такое приложение использовали участники массовых беспорядков для быстрого уведомления об аресте, когда нет времени позвонить. Однако приложение можно использовать и в «мирное время», например, для уведомления о том, что вы попали в какую-то неприятную ситуацию. Как только вы нажмете тревожную кнопку, ваши друзья узнают, что с вами случилась беда.

Приложение очень простое и, в отличие от предыдущего, содержит только тревожную кнопку и возможность добавления номеров телефонов, на которые будут отправлены SMS. Текст сообщения нужно ввести заранее, как и номера телефонов (указываются через запятую). В тексте представьте максимум информации о том, где вы можете быть, что собирались сделать и т. д. — тогда вашим близким станет понятно, что с вами случилось и где вас искать. Никакой дополнительной информации типа GPS-координат в SMS содержаться не будет. На рис. 8.4 показано приложение I'm Getting Arrested в действии.

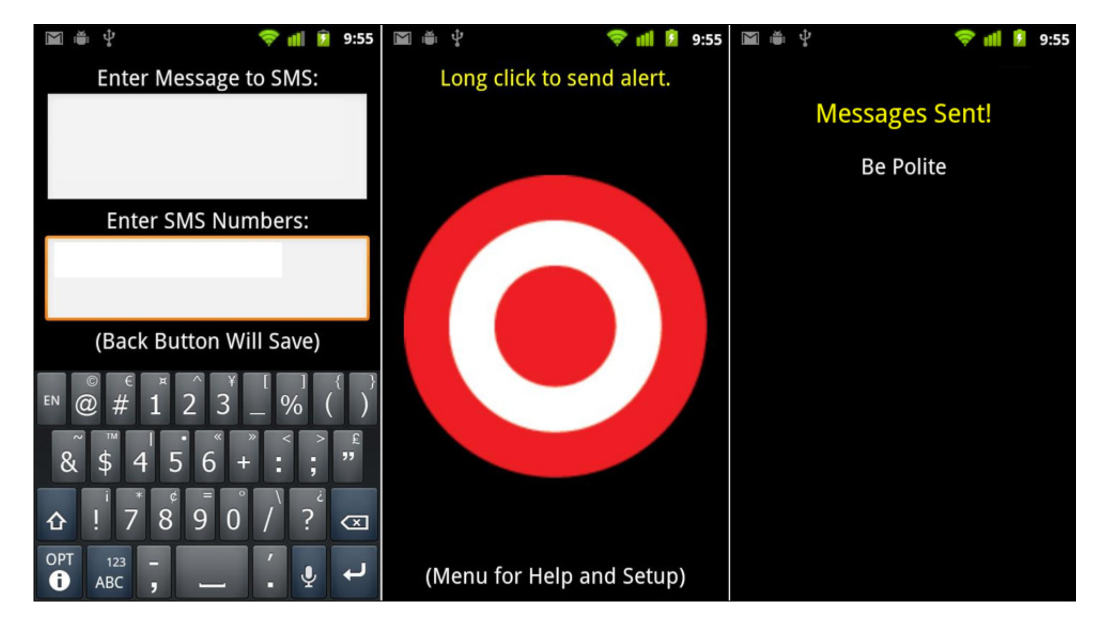


Рис. 8.4. Приложение I'm Getting Arrested

Установить приложение можно по ссылке:

https://play.google.com/store/apps/details?id=us.quadrant2.arrested

8.4. Запись телефонного разговора

В жизни случаются ситуации, когда нужно записать телефонный разговор. Причины этой необходимости могут быть различны: от элементарной забывчивости (если ею страдаете вы или ваш собеседник) до угроз в ваш адрес. Случается и такое, что человек говорит одно, а потом пытается убедить вас, что говорил совсем другое. Тут на помощь и придет запись телефонного разговора.

Всех юридических тонкостей сего процесса я не знаю, но, насколько помню, по закону ваш собеседник должен быть предупрежден о том, что ведется запись разговора. Однако иногда (в случае тех же угроз) такое предупреждение просто не имеет смысла.

Программы для записи переговоров есть для всех мобильных платформ, а для Android лучшей программой на сегодняшний день является Запись звонков (Total Recall), ссылка на нее на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.killermobile.totalrecall

Обратите внимание, что существуют версии этой программы для разных устройств. Так, для смартфонов Sony Xperia и Samsung Galaxy S II и S III имеются свои версии, соответственно:

https://play.google.com/store/apps/details?id=com.killermobile.totalrecall.x10.trial

https://play.google.com/store/apps/details?id=com.killermobile.totalrecall.s2.trial

Программа очень проста в использовании — вы запускаете ее и забываете о ней, она не мешает в работе, а индикация в строке состояния подскажет, что разговор в данный момент записывается.

Как и все такого рода программы, Запись звонков имеет весьма гибкие настройки, в том числе вы можете выбрать несколько форматов сжатия звука. Но более всего мне понравилась возможность включения записи через микрофон при получении на телефон секретной SMS. Вас просят выйти, но вы хотите быть в курсе событий? Вы выходите, но как бы нечаянно забываете в помещении телефон. Затем с другого номера отправляете на него SMS, и программа Запись звонков начинает записывать ведущиеся в помещении разговоры. Вернувшись, вы забираете свой телефон и прослушиваете запись. Правда, настоящая находка для шпиона?

Казалось бы, вот оно, идеальное решение. Но в этом мире нет ничего идеального, и программа Запись звонков тоже не исключение из правил. Первый ее недостаток — это цена! На фоне других приложений, которые стоят 2–3 доллара, эта программа стоит целых $10, что очень дорого для Android-приложения. Впрочем, есть и бесплатная ограниченная версия этой программы. Сначала установите ее, чтобы убедиться, что программа будет работать на вашем телефоне.

Дело в том, что у программы есть и второй недостаток — на некоторых телефонах она не работает, поэтому бесплатная версия будет весьма кстати. По крайней мере, вы узнаете, сможет ли программа записывать разговоры именно на вашем устройстве.

К тому же, программа ведет запись голоса только через микрофон. Казалось бы, а что тут такого? Но когда вам захочется подключить к телефону гарнитуру для более качественной записи, программа ваш голос записать не сможет.



ГЛАВА 9

Некоторые полезные системные приемы

9.1. Удаление рекламы из приложений

Рекламу часто называют двигателем торговли. Однако двигатель она для одних, а для других — раздражитель. Да, для тех, кто предлагает свои товары (все равно что — будь то таблетки, гарантирующие исцеление от всех болезней, или новая программа), реклама — это двигатель торговли. А вот для нас, потребителей, она постоянный раздражитель. Смотришь фильм, он прерывается на самом интересном месте, бац — рекламная пауза. Бороздишь сайты — везде пестрящие баннеры, занимающие на маленьком экране телефона слишком много места, а если еще и 3G-трафик платный, то вам предлагается разглядывать их за свой счет.

Способ избавиться от надоедливых рекламных баннеров для «больших» компьютеров давным-давно найден, есть он и для Android, так что мы тоже можем избавиться от рекламы внутри Android-приложений. Конечно, способ этот довольно-таки грубый, но проверенный. Прежде, чем продолжить, предупреждаю, что все действия вы выполняете на свой страх и риск! Если не хотите рисковать, покупайте платные версии приложений — они, как правило, позволяют обходиться без рекламы.

Итак, поможет избавиться от рекламы абсолютно бесплатная программа AdFree Android, вы без особых проблем найдете ее на Google Play Маркет.

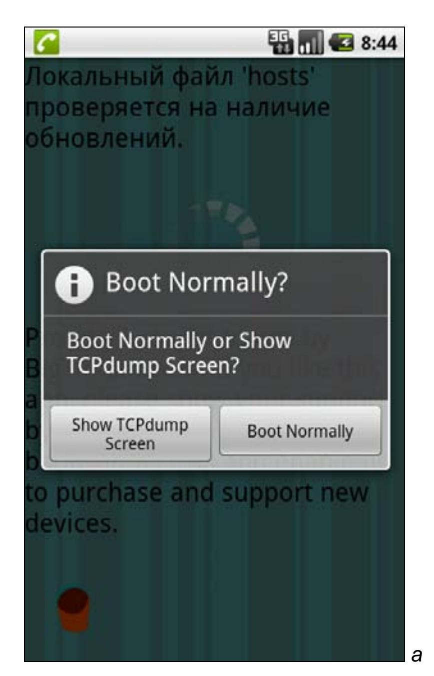
Использовать программу очень просто — при первом запуске она спросит вас, как загружаться? Нажмите кнопку **Boot Normally** (рис. 9.1, *а*), а затем кнопку **Загрузить и Установить Имена** (рис. 9.1, *б*). Осталось только перезапустить программы, в которых присутствовала реклама, или перезагрузить телефон.

Рекламы вы больше не увидите, причем не только в приложениях, но и в Интернете. На месте рекламы в браузере появится сообщение **Страница не загружена**. Если появится желание вернуть все, как было, запустите программу и нажмите кнопку **Восстановить Оригинал**.

Принцип работы программы элементарен — она подменяет системный файл hosts модифицированным, где изменены IP-адреса для загрузки рекламы. Теперь реклама должна была бы загружаться с вашего телефона (127.0.0.1), а так как ее там нет и

быть не может, то она вовсе не станет загружаться. В итоге рекламные сообщения не только перестанут вас раздражать, но вы еще и сэкономите трафик.

В общем-то, проделанную программой работу можно выполнить и вручную, без привлечения программы, но вам придется найти где-то измененный файл hosts — вы же не будете прописывать в нем все адреса вручную. Кроме того, для этого нужно еще знать, откуда программы загружают рекламу. Так что намного проще установить программу и наслаждаться ее работой. К тому же AdFree регулярно обновляет адреса в базе рекламы, следовательно, автоматически обновляется и ваш файл hosts, и как только появятся новые ресурсы с рекламой, они тут же будут внесены в базу AdFree.



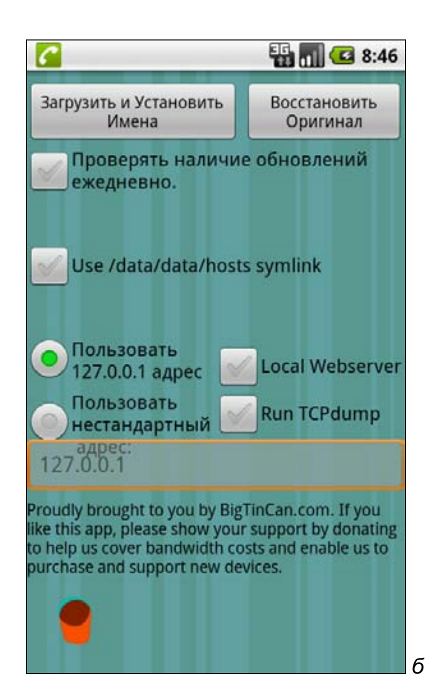


Рис. 9.1. Запуск AdFree: *а* — кнопка **Boot Normally**;
б — кнопка **Загрузить и Установить Имена**

Программу AdFree можно удалить сразу после использования, а заново установить, только когда опять в приложениях начнет появляться реклама. Программа запишет в систему обновленную версию файла hosts, и ее опять можно будет удалить, чтобы не захламлять телефон.

Почему я назвал этот способ грубым? Нет, мне не жалко рекламы. Просто программа для своей работы требует права root, а процесс получения этих прав часто бывает опасным для телефона. Другими словами, в попытке избавиться от рекламы вы можете испортить свой телефон. Использовать эту программу или нет — решайте сами.

Получение полномочий root

Процесс получения полномочий root отличается для разных телефонов и подробно описан в *главе 10*.

Есть и другой способ избавиться от рекламы в приложениях, он не универсальный, зато не требует прав root. В *главе 3* была рассмотрена программа NoRoot Firewall, позволяющая закрыть доступ к Интернету определенным приложениям. Представим, что у нас есть программа, не требующая доступа к Интернету, — например, какая-то несетевая игра, программа-планировщик и т. п. Такой программе, по сути, доступ к Интернету не нужен, а Интернет она использует для одной цели — для загрузки рекламы. В этом случае с помощью NoRoot Firewall можно запретить такой программе доступ к Интернету без потери основной функциональности.

Однако, как было отмечено, этот способ не универсальный. Во-первых, он не позволяет избавиться от рекламы, если приложению нужен доступ к Интернету для выполнения основной функциональности — например, это клиент обмена мгновенными сообщениями. Запретив такой программе доступ к Интернету, вы перекроете путь рекламе, но и программа перестанет работать, как надо.

Во-вторых, если у вас установлено множество отображающих рекламу программ, которым доступ к Интернету не нужен, запрещать его придется отдельно для каждой программы. Впрочем, таких программ вряд ли будет много, стало быть это не вызовет для вас каких-либо неудобств — один раз настроили брандмауэр и забыли.

9.2. Удаление рекламы из области уведомлений

Только что мы разобрались, как убрать рекламу из Android-приложений, а сейчас поговорим об удалении рекламы из области уведомлений. Такая реклама не только раздражает, но и попросту вредна. Если реклама в Android-приложениях не выходит за рамки этих приложений, то реклама в области уведомлений может стать причиной того, что вы пропустите важное уведомление, поскольку она очень быстро захламляет эту самую область. В результате вы можете не увидеть уведомление о новом, важном для вас сообщении e-mail или еще что-то нужное. К тому же ссылки, появляющиеся в области уведомлений, могут указывать на вредоносные приложения, что очень плохо.

Рекламные сообщения попадают в область уведомлений благодаря технологии AirPush. Для обнаружения приложения, которое «спамит», можно использовать программу AirPush Detector. Она быстро вычислит «врага», после чего вы можете или покопаться в настройках этой программы и отключить рекламу, или же просто ее удалить. Отмечу, что в большинстве случаев придется удалить программу.

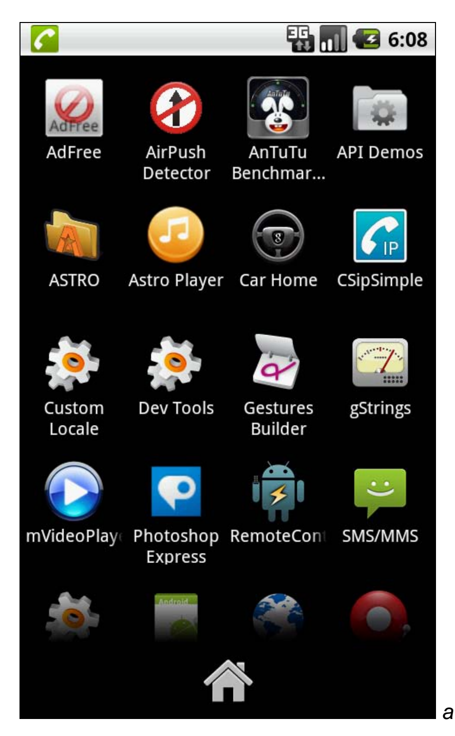
Программа AirPush Detector абсолютно бесплатна, и для ее работы не нужны полномочия root. Установить программу можно по ссылке:

https://play.google.com/store/apps/details?id=com.brosmike.airpushdetector

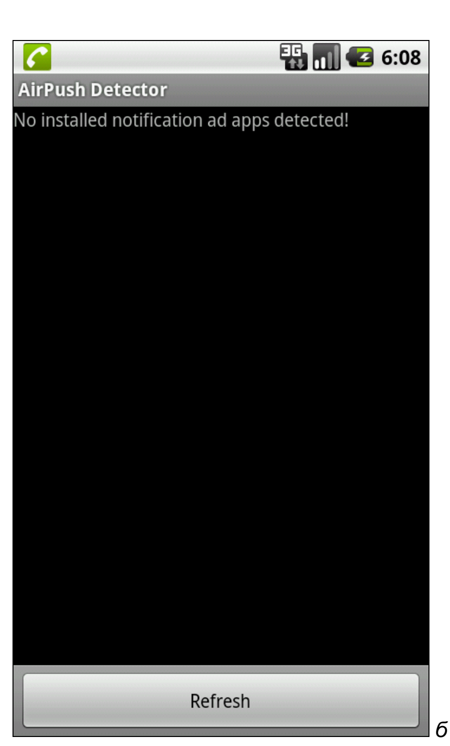
После установки значок программы появится рядом со значком AdFree (рис. 9.2, *а*), если, конечно, вы ранее установили эту программу. Запустите AirPush Detector и получите список приложений, отправляющих рекламу в вашу область уведомле-

ний. В моем случае таких приложений не оказалось, чего, собственно, и следовало ожидать (рис. 9.2, *б*).

Обладателям устройств с Android версии 4.1 (не 4.0) или более новой эта программа не нужна, поскольку вся необходимая функциональность обеспечивается самой системой. Нажмите пальцем на рекламу и удерживайте палец, пока система сама не сообщит, какое приложение отправило уведомление.



а



б

Рис. 9.2. Программа AirPush Detector: *а* — значок **AirPush Detector**; *б* — нет приложений, отправляющих рекламу в область уведомлений

Примечание

В отличие от AdFree, программа AirPush Detector не требует прав root, поэтому использовать ее можно без всяких последствий для телефона. Она просто сообщит, какие приложения «спамят», а что делать с ними — решайте сами: их можно завершить или вообще удалить (через меню **Управление приложениями**).

9.3. Избавляемся от рекламы при просмотре сайтов

К сожалению, рекламы в Интернете становится все больше, и она становится все более навязчивой. На настольных системах можно использовать специальные утилиты, блокирующие рекламу. Для Android толковых утилит подобного плана пока мало, но они есть. Одна из самых лучших (если не самая лучшая) — AdBlock. Ути-

лита блокирует баннеры, всплывающие окна и видеорекламу — даже на Facebook и YouTube. При этом ненавязчивые объявления блокироваться не будут — ведь сайты, на которых размещены никому не мешающие рекламные объявления, тоже нужно поддерживать.

Программа очень эффективна и при этом абсолютно бесплатна. Однако видимо потому, что она блокирует рекламу Facebook и YouTube, ее исключили из Play Маркет. Но не расстраивайтесь, программу можно скачать с сайта разработчиков:

https://adblockplus.org/ru/android

Перед установкой программы включите установку приложений из неизвестных источников (это можно сделать в разделе меню **Безопасность** страницы настроек), скачайте и установите APK-файлы программы.

Программа не только убирает навязчивые объявления, но и экономит ваши нервы и ваш трафик.

9.4. Файловый менеджер

Как ни странно, но в Android нет штатного файлового менеджера. Свой файловый менеджер есть даже в Bada OS, а вот в Android — нет (исключения составляют устройства от Samsung, но наличие в них файлового менеджера — это заслуга Samsung, а не разработчиков Android). Видимо, разработчики Android хотят оградить пользователя от путешествий по файловой системе.

Зато разработчики приложений для Android с удовольствием заполнили этот пробел в программном обеспечении. На Google Play Маркет вы можете найти множество самых разных файловых менеджеров — и платных, и бесплатных. Самые известные из них: Astro File Manager, ES Проводник, Total Commander. Первая программа устраивала меня до тех пор, пока я не установил ES Проводник, которая мне показалась более удобной. Программа Total Commander — аутсайдер на фоне первых двух программ по своим возможностям. Да, двухпанельный интерфейс лично для меня весьма удобен, но в программе нет и половины тех возможностей, которые есть в ES Проводник. Вы можете установить все эти три программы (они, кстати, бесплатные) и выбрать ту, которая вам больше всего понравится, а сейчас мы рассмотрим ES Проводник, установить которую можно по ссылке:

https://play.google.com/store/apps/details?id=com.estrongs.android.pop

Использовать программу довольно просто, и если вы знакомы с обычным Проводником Windows, то без проблем разберетесь и с ES Проводник. На рис. 9.3 изображен основной экран программы — содержимое внутренней карты памяти. Именно этот экран откроется сразу после запуска программы. В нижней части окна вы увидите следующие кнопки:

- **Создать** — кнопка создания файла или каталога;
- **Поиск** — поиск файлов на вашем устройстве;
- **Обновить** — обновление текущей области;

- **Вид** — изменение представления текущей области;
- **Окна** — каждое расположение ES Проводник открывает в отдельном окне, список окон как раз можно просмотреть, нажав эту кнопку.

Рис. 9.3. Программа ES Проводник

Рис. 9.4. Основные действия над выделенными объектами

Для выделения файлов или каталогов нужно нажать и удерживать значок файла/каталога, пока на нем не появится флажок, свидетельствующий о том, что этот файл/каталог выделен. После выделения первого файла/каталога в нижней части окна программы (рис. 9.4) появятся кнопки **Копировать** (копирование выделенных объектов в буфер обмена), **Вырезать** (используется для перемещения объектов), **Вставить** (вставить объекты из буфера обмена в текущее расположение), **Переименовать** (переименование выделенного объекта), **Удалить** (удаление выделенных объектов). Доступна здесь также и кнопка **Еще**, отображающая меню с дополнительными действиями над выделенными объектами (рис. 9.5).

В меню этой кнопки вы найдете действия открытия файла в альтернативной программе (**Открыть как**), отправки файла (**Отправить**), сжатия файла (**Сжать**), отображения окна свойств файла (**Свойства**) и т. д.

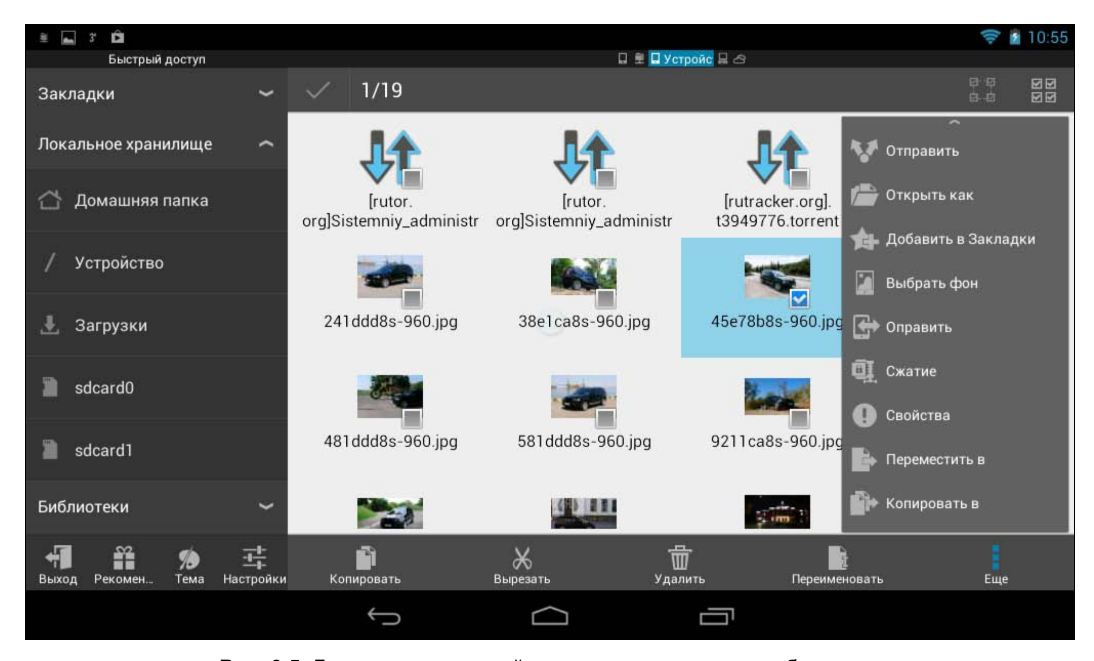


Рис. 9.5. Дополнительные действия над выделенными объектами

9.5. Восстановление удаленных файлов

Восстановить случайно удаленный файл с SD-карты Android-устройств можно с помощью любой программы, позволяющей восстанавливать файлы с флешки или SD-карты. Таких программ очень много, и вы можете выбрать любую. Как правило, эти программы работают под управлением Windows. Вам нужно извлечь SD-карту из устройства, вставить ее в специальный microSD-переходник, а затем — в кард-ридер ноутбука или стационарного компьютера. Далее можно запустить любую программу для восстановления карты памяти — например, CardRevocery или iCare Data Recovery.

Совсем другое дело, когда файлы находятся на внутренней карте памяти устройства, и ее нельзя извлечь. В этом случае файлы можно восстановить программой 7-Data Recovery, скачать которую можно по ссылке:

http://7datarecovery.com/android-data-recovery/

Программа совершенно бесплатна и, похоже, единственный ее недостаток — наличие только Windows-версии. К сожалению, версий для других операционных систем нет, и если вы владелец MacBook'а, вам придется искать друга, имеющего компьютер под управлением Windows.

Алгоритм использования этой программы прост:

1. Запустите программу.
2. Включите отладку по USB (см. об этом в *главе 10*) и подключите устройство к компьютеру.
3. В программе 7-Data Recovery нажмите кнопку **Далее**.
4. Выберите внутреннюю SD-карту и нажмите кнопку **Далее**.
5. Выберите файлы, которые нужно восстановить, и нажмите кнопку **Сохранить**.

Нужно отметить, что восстановить получится файлы не со всех устройств — некоторые не поддерживают такой метод восстановления. Но попытаться стоит — хуже вы точно не сделаете.

9.6. Экономия заряда аккумулятора

Читая эту книгу, вы установили на свой смартфон (планшет) много полезных программ. Но дело в том, что теперь все эти программы (например, VPN-клиент, Orbot, AppLock и т. д.) начинают потреблять системные ресурсы, и аккумулятор вашего устройства разряжается быстрее.

Далее приведены простые рекомендации, придерживаясь которых, вы сможете продлить время автономной работы устройства.

- **Тщательно заряжайте аккумулятор**. Не насилуйте его частыми зарядками по 10–15 минут. Лучше дождаться практически полного его разряда, а затем зарядить полностью. В зависимости от модели смартфона на полную зарядку аккумулятора понадобится 4–5 часов, поэтому лучше всего поставить телефон на зарядку на ночь.
- **Выключайте Bluetooth**, когда им не пользуетесь.
- **Отключайте Wi-Fi, когда не пользуетесь Интернетом**, даже если вы находитесь в зоне действия Wi-Fi. Бывает так, что вы уже вышли за пределы действия Wi-Fi, но забыли выключить адаптер, и он продолжает искать доступные сети, что очень быстро «сажает» аккумулятор.
- **Установите минимальное время отключения экрана** — скажем, 15 секунд.
- **Установите минимальную яркость дисплея** или хотя бы 50-процентную. В помещении этого будет вполне достаточно, а на солнце, что при 50 % яркости, что при 100 % — видно плохо.

- **Используйте стандартную тему оформления смартфона**. Она хоть и не такая «навороченная» и красивая, как темы сторонних разработчиков, зато позволяет экономить заряд аккумулятора.
- **Отключите анимационные эффекты** в настройках телефона. Использование стандартной темы оформления и отключение анимационных эффектов позволит отвоевать до 30 дополнительных минут работы вашего устройства.
- **Отключите лишние программы** — например, виджеты. Каждая запущенная программа потребляет системные ресурсы, следовательно, создает нагрузку на железо и разряжает аккумулятор.
- **Забудьте об анимированных или так называемых *активных* заставках**, загружающих информацию из Сети. Установите в качестве заставки обычную фотографию — этим вы существенно сэкономите заряд аккумулятора.
- **Если нужно протянуть хотя бы еще часик**, отключайте все: Интернет, Bluetooth, Wi-Fi, закрывайте все программы, виджеты, экран — на минимальную яркость. Так устройство протянет лишний час в режиме ожидания. А вдруг за это время состоится важный звонок? Так вы сможете хотя бы несколько минут поговорить, прежде чем устройство окончательно выключится.
- **Старайтесь избегать переохлаждения устройства**. Это вредно как для аккумулятора, который теряет заряд на морозе, так и для самого устройства, где при резком перепаде температур образовывается конденсат. Старайтесь носить телефон во внутреннем кармане, а не в портмоне или в сумочке (это особенно касается девушек). Планшет вообще лучше отключать при выходе на сильный мороз, а войдя в помещение включать его не сразу — пусть пройдет хотя бы полчаса. Вообще-то так следует обращаться и со смартфоном, но мало кто захочет пропускать звонки из-за возможного образования конденсата.

Если приведенные рекомендации вам не помогли, тогда нужно выяснить, какая программа расходует заряд больше всех. В этом вам поможет приложение Power Tutor, абсолютно бесплатно скачать которое можно по ссылке:

https://play.google.com/store/apps/details?id=edu.umich.PowerTutor

Принцип работы программы прост — она сообщает, какое приложение больше всего нагружает процессор телефона и, следовательно, больше всех «съедает» заряд (рис. 9.6). Для полноценной работы программы нужны права root.

> ***Права root***
>
> Что такое права root и как их получить, вы сможете узнать из *главы 10*. Здесь же кратко поясню, что root — это администратор телефона, права которого устанавливаются особым образом. А вы, владелец телефона, являетесь всего лишь рядовым его пользователем. Это все так организовано, исходя из принципа «не навреди».

Что делать, получив информацию о наиболее прожорливых процессах? Все зависит от выполняемых процессов. Если это пользовательское приложение — например, виджет погоды, его можно просто завершить, и оно больше не будет разряжать ак-

кумулятор. Если же его сажает системная программа, придется смириться или искать решение на разных форумах, поскольку конкретное решение зависит от многих факторов — процесса, версии Android, самого телефона и т. д.



Рис. 9.6. Программа Power Tutor



ГЛАВА 10

На свой страх и риск

Все действия, которые вы будете выполнять над своим телефоном, следуя указаниям из этой главы, вы выполняете на свой страх и риск. Вы должны отдавать себе отчет — получение полномочий root, в том числе их неправильное использование, может превратить ваш современный смартфон из последнего чуда техники в ни на что не способный «кирпич».

10.1. Что такое root-доступ?

Что такое root-доступ, UNIX/Linux-пользователям объяснять не нужно. Они прекрасно понимают, что это, и почему root-полномочия потенциально опасны для системы (в неумелых руках). Здесь же я попробую объяснить, что такое root, обычному человеку, не знакомому с тайнами UNIX.

Итак, несколько упрощая, отметим, что в системе могут быть два типа пользователей: администратор (или администраторы, если их несколько) и самые обычные пользователи. Выполнение системных действий требует полномочий администратора. В UNIX и Android администратор, обладающий неограниченными полномочиями, и называется root.

Соответственно, телефон на базе Android изначально предоставляет своему хозяину далеко не все права, поскольку считает его обычным пользователем. А у обычного пользователя нет доступа к системному разделу, и чтобы его получить, нужны полномочия root.

Учитывая, что далеко не все покупатели телефонов являются гуру Android, такой подход весьма оправдан, иначе бы каждое второе устройство практически сразу попадало бы в сервисный центр. Ведь неопытный пользователь с root-правами может нечаянно удалить какой-то важный системный файл, и его новейший смартфон превратится в никому ненужный «кирпич».

Root-доступ в Android отличается от root-доступа в UNIX, поскольку в Android для пользователя root просто открывается системный раздел — становится возможным читать имеющиеся на нем файлы и записывать в него какие-то свои.

Сами системные файлы Android интересны мало, но после получения root-доступа вы можете устанавливать неофициальные прошивки, некоторые системные программы типа брандмауэра или программ резервного копирования (например, Titanium Backup), разгонять процессор и т. д. Как видите, root-доступ может быть весьма полезен, но используйте его с осторожностью, поскольку та же неофициальная прошивка не дает гарантии работоспособности телефона, а если что-то пойдет не так, в гарантийном ремонте вам откажут.

В любом случае, если вы читаете эту главу, то наверняка знаете (или, хотя бы, предполагаете), зачем вам root-доступ. Не следует пытаться его получить «лишь бы было», без всякой конкретной цели — так можно просто навредить.

Процедуры получения root-доступа различны для разных устройств. В этой главе мы рассмотрим ее для некоторых популярных смартфонов. Сами понимаете, описать эту процедуру для всех смартфонов невозможно. Если у вас другое устройство, а root-доступ все-таки нужен, постарайтесь найти подробные инструкции в Интернете — они наверняка отыщутся.

Запомните только одно — если вы не понимаете, зачем вам root-доступ, или сомневаетесь в своих знаниях, умениях и навыках, лучше перейдите к чтению следующей главы. И не говорите, что я вас не предупреждал!

10.2. Необходимые программы

Обычно для получения root-доступа нужно скачать и установить специальную программу. После этого вы ее запускаете, нажимаете кнопку **Root** (или подобную), через некоторое время телефон перезагружается, и вы получаете полную власть над ним. Такие специальные программы, понятное дело, вы не найдете на Google Play Маркет.

Архив необходимых программ

Для большего вашего удобства все программы, описанные в этой главе, я собрал и поместил в один архив, который совершенно бесплатно можно скачать из раздела **Downloads** (рис. 10.1) моего сайта, расположенного по адресу: **http://www.dkws.org.ua/f/downloads**.

Конечно, все программы этого архива вам не понадобятся, но, вполне вероятно, что потренировавшись на своем телефоне, вы потом захотите помочь в получении прав root своим друзьям и коллегам, поэтому в архив и помещено практически все необходимое.

Почему «практически» все? Да потому что для получения root-доступа кроме программ нужны также драйверы для конкретных телефонов и, в некоторых случаях, так называемые *небезопасные ядра*. Понятно, что я не могу собрать абсолютно все драйверы для всех телефонов. Вам нужно найти их в Интернете самостоятельно или установить Android SDK — в нем есть много драйверов для самых разных устройств. Но пока об этом не беспокойтесь — все станет ясно при дальнейшем чтении. То же касается и небезопасных ядер, которые понадобятся, к счастью, не для

Downloads

На сайте залито много интересных и полезных файлов, но найти тот или иной файл становится сложно, поскольку приходится перелопачивать форум, курить поиск Google. Попытался собрать все воедино на этой страничке. Щелкаем правой кнопкой по ссылка и выбираем команду **Сохранить по ссылке как**.

Android

Программы, необходимые для получения root

Листинги к книгам

Все значимые листинги для "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1

Листинги для гл. 34 "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1/2 (FIXED)

Листинги для гл. 34 "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1/2 (FIXED)

Листинги для гл. 15 "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1/2

Листинги для гл. 31 "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1

Листинги для гл. 33 "PHP 5/6 и MySQL 6. Разработка Web-приложений", издание 1

Рис. 10.1. Раздел **Downloads** сайта **dkws.org.ua**

всех телефонов. Адрес ссылки, откуда можно будет скачать эти ядра, также будет предоставлен далее.

Для получения root-доступа мы воспользуемся следующими программами:

- GingerBreak — устанавливается непосредственно на сам телефон;
- SuperOneClick — устанавливается на компьютер, телефон подключается к компьютеру по USB;
- Unlock Root — как и SuperOneClick, устанавливается на компьютер. Программа поддерживает огромное число устройств, далее будет приведена ссылка на список таких устройств;
- z4root — как и программа GingerBreak, эта программа устанавливается в ваш телефон, откуда и производит все необходимые манипуляции.

Конечно, это далеко не все существующие для «рутования» программы. В Интернете есть много других программ, которые также можно использовать.

А теперь рассмотрим перечисленные программы с точки зрения поддерживаемых ими устройств. Начнем с GingerBreak. Вот список устройств, поддерживаемых программой GingerBreak (в скобках — версия Android и/или дополнительные условия работы программы):

- Alcatel OT-890D (2.2.2);
- Acer Liquid (2.2);
- Acer Liquid MT (2.2);
- apad imx515 (2.3.3);
- Dell Streak (2.2.2);
- Desire HD (2.3.3, S-OFF);
- HTC Desire S, Incredible S (S-OFF);
- Google Nexus One (2.3.3);
- Highscreen Cosmo;
- Huawei U8800 (2.2.1);
- Huawei S7 (2.2);
- LG Optimus 2X (stock);
- LG Optimus Black (2.2.2);
- LG Optimus One (2.2.1);
- LG P 350 (2.2.2);
- Motorola Defy;

- Nexus S (2.3.3);
- Samsung GT-I9003 Galaxy S scLCD (2.2.1);
- Sony Ericsson Arc;
- Sony Ericsson Neo, 2.3.2;
- Sony Ericsson Xperia Play;
- SGS (2.3.3);
- ViewSonic 10s (2.2);
- ViewSonic Viewpad7 (2.2).

Отмечу, что программой GingerBreak не на всех этих устройствах можно получить root-доступ, а на некоторых устройствах получение root-доступа очень даже опасно — есть большая вероятность, что что-то пойдет не так! Приведу список таких устройств (группа риска):

- Samsung Galaxy Ace;
- Samsung Galaxy Mini;
- HTC Desire S;
- HTC Wildfire;
- HTC Incredible S (2.3.3);
- SE Xperia Neo (2.3.3);
- SGS (2.3.3).

Посмотрите — устройство Desire S от HTC, например, присутствует в обоих списках. Да, для него можно использовать программу GingerBreak, но в то же время может возникнуть и неприятность. Так что будьте осторожны с этой моделью телефона.

Теперь перейдем к программе SuperOneClick. Она поддерживает следующие аппараты:

- HTC серии Desire;
- HTC Aria;
- HTC Legend;
- HTC Wildfire (HTC Buzz);
- HTC Magic (Sapphire) 32B;
- HTC Bee;
- Droid Eris (HTC Desire C);
- Droid Incredible (HTC Incredible);
- Sprint EVO 4G (HTC Supersonic);
- Acer Liquid Metal;
- Dell Streak;
- LG (все модели);
- Motorola Atrix4G;
- Motorola Charm;
- Motorola Cliq;
- Motorola Droid;
- Motorola Flipside;
- Motorola Flipout;
- Motorola Milestone;
- Nexus One;
- Samsung Captivate;
- Samsung Galaxy 551 (GT-I5510);
- Samsung Galaxy Portal/Spica I5700;
- Samsung Galaxy S 4G;
- Samsung Galaxy S I9000;
- Samsung Galaxy S SCH-I500;
- Samsung Galaxy Tab;
- Samsung Transform M920;
- Samsung Vibrant;
- Sony Ericsson Xperia E51i X8;
- Sony Ericsson Xperia X10;
- Sprint Hero;

- Telus Fascinate;
- Toshiba Folio 100;
- T-Mobile G2;
- T-Mobile MyTouch 3G 32A (v1.2);
- T-Mobile MyTouch 4G.

На некоторых телефонах из этого списка включена защита (S-ON). Чтобы воспользоваться программой SuperOneClick, нужно сначала снять защиту (получить S-OFF), а уже потом запустить программу. Вот список таких устройств (это HTC и их производные):

- Sprint EVO 4G (HTC Supersonic);
- Droid Incredible (HTC Incredible);
- HTC Desire GSM;
- HTC Desire CDMA (HTC BravoC);
- HTC Aria;
- Droid Eris (HTC DesireC);
- HTC Wildfire (HTC Buzz).

Программа Unlock Root, наверное, наиболее универсальна. Далее будет приведена ссылка на список поддерживаемых устройств. Также отмечу, что она поддерживает все современные версии Android: от 2.1 до 4.0.

Программа z4root не так универсальна, как Unlock Root, но в некоторых случаях ее очень удобно использовать. Вот список поддерживаемых ею устройств:

- Acer Liquid S100;
- Cricket Huawei Ascend;
- Garmin-Asus A10;
- Gigabyte GSmart 1305;
- HTC Hero (Android 2.1);
- Huawei U8110;
- Huawei U8150 (Android 2.2);
- Huawei U8220;
- Huawei U8230;
- Huawei U8500;
- LG GT540 (2.1);
- LG P500 Optimus One (Android 2.2);
- Motorola Backflip;
- Motorola Defy;
- Motorola Droid X;
- Motorola Droid 1 (Android 2.2.1);
- Motorola Droid 2;
- Motorola Quench XT5;
- Pocketbook IQ 701;
- Samsung Acclaim;
- Samsung GT-I5700 Spica;
- Samsung GT-I5800 Galaxy 3;
- Samsung GT-I7500 Galaxy;
- Samsung GT-I9000 Galaxy S (строго до Android 2.2.1);
- Samsung GT-P1000 Galaxy Tab;
- Sony Ericsson X10;
- Sony Ericsson X10 mini;
- Sony Ericsson X10 mini pro;
- SuperPad (WowPad / Fly Touch II) Infotm x220.

А вот на этих устройствах программу z4root использовать не рекомендуется (или она используется с ограничениями):

- Archos 70;
- Google Nexus One;

- HTC Desire (требует S-OFF, после чего можно использовать);
- HTC Desire HD (требует S-OFF, после чего можно использовать);
- HTC Droid Incredible;
- HTC Evo (требует S-OFF, после чего можно использовать);
- HTC Legend;
- HTC Magic (требует S-OFF, после чего можно использовать);
- HTC Wildfire;
- T-Mobile G2 (требует S-OFF, после чего можно использовать);
- T-Mobile MyTouch 3G;
- Motorola Droid1;
- Samsung GT-I9000 Galaxy S (только с Android 2.2.1);
- Sony Ericsson X8 (только Android 2.1).

Отмечу теперь несколько особенностей всех Windows-программ:

- поскольку платформа Android достаточно молодая, то на компьютерах с Windows XP вам придется установить Microsoft .NET Framework 2.0 или даже 4.0. Благо, это чудо технической мысли можно бесплатно скачать с сайта Microsoft. Ссылку вы найдете с помощью поиска Google;
- в Windows Vista и Windows 7 программы нужно запускать от имени администратора. Для этого щелкните на исполнимом файле правой кнопкой мыши и выберите команду **Запуск от имени администратора**;
- хотя одну и ту же программу можно использовать для «рутования» разных телефонов, последовательность действий может немного отличаться, в чем вы убедитесь при чтении этой главы. Так что у каждого телефона есть свои особенности и секреты. Вполне возможно, что программа будет отлично работать с одной версией прошивки, а с другой — откажется.

10.3. «Рутование» устройств

10.3.1. Смартфоны LG Optimus One и LG Optimus 2X

Получим на смартфонах LG Optimus One (рис. 10.2) и LG Optimus 2X (рис. 10.3) root-доступ с помощью программы GingerBreak, которая включена в состав архива, упомянутого в *разд. 10.2*.

Иллюстрации этой главы

Зачем в этой главе фотографии устройств? Да просто для разряжения обстановки. Если вы захотели прочесть всю главу одним махом, то от всех тонкостей рискуете получить настоящий «взрыв мозга». Так что, когда устанете, просто посмотрите картинки ☺.

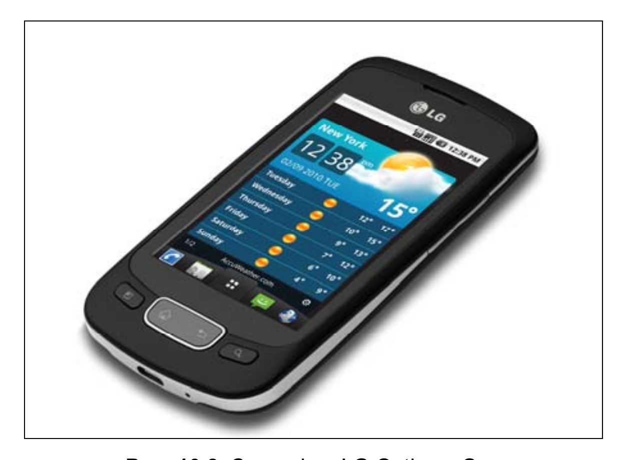



Рис. 10.2. Смартфон LG Optimus One



Рис. 10.3. Смартфон LG Optimus 2X

Общая последовательность действий следующая:

1. Установите GingerBreak.
2. Включите отладку по USB (**Настройки | Приложения | Разработка | Отладка USB**). Перед этим в устройство должна быть установлена флешка.
3. Запустите GingerBreak (рис. 10.4) и выберите LG Optimus 2X.
4. Подождите, пока устройство перезагрузится. Ждать придется долго, не нужно думать, что устройство зависло, и принудительно выключать его — иначе в результате точно получите «кирпич».

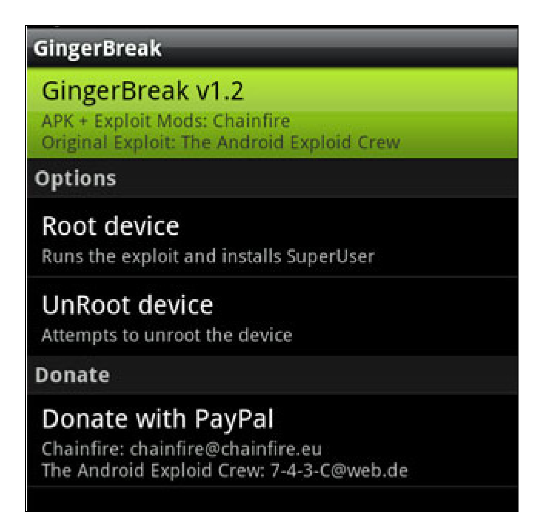


Рис. 10.4. Программа GingerBreak

После этого, если вам повезет, вы получите root-доступ. Если не повезет — не получите. Скорее всего, с LG Optimus One все будет нормально, а вот с LG Optimus 2X все зависит от версии Android. Если на устройстве установлена Android 2.2, то можно без проблем использовать GingerBreak. Совсем другое дело — если версия Android 2.3. Там GingerBreak уже не сработает, и следует запускать другую утилиту — SuperOneClick. Но использовать ее надо иначе. То есть если GingerBreak нужно было устанавливать на телефон, то SuperOneClick устанавливается на компьютер, к которому подключается телефон. Другими словами, одним смартфоном не обойтись, понадобится еще и компьютер.

SuperOneClick и некоторые антивирусы!

Некоторые антивирусы (в том числе Касперский) видят в SuperOneClick вирус, поэтому перед ее запуском (точнее, перед распаковкой архива) лучше антивирус временно отключить.

Перед тем как приступить непосредственно к самому процессу получения root-доступа, компьютер требуется подготовить. Так, если вы до сих пор работаете в Windows XP, следует установить Microsoft .NET Framework 2.0 или выше (скачать его можно с сайта Microsoft). Затем нужно будет установить драйверы для связи компьютера с телефоном через ADB (Android Debug Bridge, дословно: «отладочный мост для Android», а по смыслу: интерфейс для отладки Android). Для устройств LG вы найдете эти драйверы в архиве LGUnitedMobileDriver_S498MA21_WHQL_ML_Ver_2.1.zip, который включен в состав того самого архива со специальными программами, упомянутого в *разд. 10.2*.

Если же вы занимаетесь разработкой Android-приложений и установили Android SDK Tools, тогда все необходимые драйверы, как правило, уже будут в системе установлены.

Вот теперь можно приступать к «рутованию». Переведите телефон в режим отладки: **Настройки | Приложения | Разработка | Отладка USB** (или **Settings | Application Settings | Development | USB Debugging**). Включив режим отладки, подождите немного и выключите этот режим. Затем, убедившись, что опция **Отладка USB** выключена, подключите телефон к компьютеру.

Внимание!

Не нужно подключать телефон к компьютеру в режиме монтирования SD-карты!

Далее выполните следующие инструкции:

1. Запустите программу SuperOneClick и нажмите кнопку **Root**.
2. Дождитесь, когда приложение сообщит **Waiting for device**.
3. После этого включите на телефоне опцию **Отладка USB**.
4. Когда появится надпись **Starting ADB Server**, выключите опцию **Отладка USB**.
5. Еще раз включите и выключите режим **Отладка USB**, чтобы снова появилась надпись **Waiting for device**.

Кстати, чтобы вернуть все, как было, в приложении имеется кнопка **Unroot**. Так что можете ею воспользоваться, чтобы закрыть root-доступ (так будет безопаснее).

10.3.2. Смартфоны Samsung GT-I9000 Galaxy S и Samsung GT-I9100 Galaxy S II

Samsung GT-I9000 Galaxy S, Android 2.2 и программа SuperOneClick



Рис. 10.5. Смартфон Samsung GT-I9000 Galaxy S

Сначала займемся смартфоном Samsung GT-I9000 Galaxy S (рис. 10.5) на базе Android 2.2. Для получения root-доступа мы также воспользуемся программой SuperOneClick (рис. 10.6). Вот только последовательность действий будет чуть хитрее ранее описанной, иначе ничего не получится.

Требования к компьютеру те же:

- если используется Windows XP, то нужно установить Microsoft .NET Framework 2.0 или выше;
- антивирус Касперского следует выключить;
- необходимо установить драйверы Android. Если Android SDK уже установлен, больше ничего устанавливать не требуется. В противном случае установите драйверы отсюда: **http://developer.android.com/sdk/win-usb.html**.

Далее выполните следующие инструкции:

1. Выключите телефон и извлеките из него SD-карту. Не знаю, как влияет наличие карты на получение root-доступа именно в этом телефоне, но экспериментальным путем установлено, что описываемый способ не сработает, если SD-карта на месте.

2. Переведите телефон в режим отладки: **Настройки | Приложения | Разработка | Отладка USB**.
3. Подключите телефон к компьютеру, запустите программу SuperOneClick и нажмите кнопку **Root**. Подождите, пока устройство не будет перезагружено.

Как видите, программа одна и та же, но последовательность действий несколько иная.

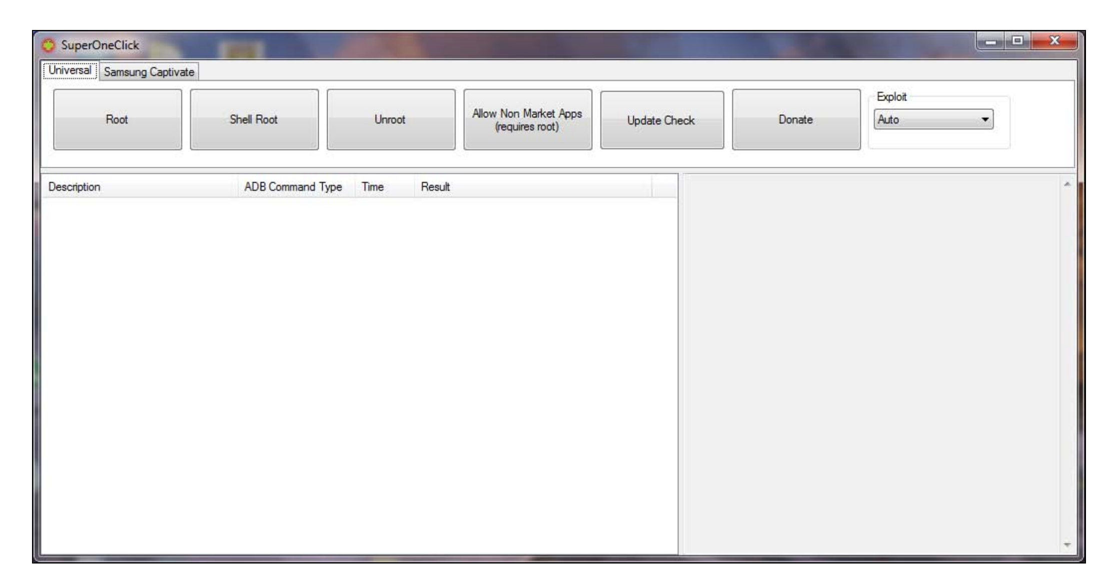


Рис. 10.6. Программа SuperOneClick

Samsung GT-I9000 Galaxy S, Android 2.3 и программа Unlock Root

Если в смартфоне Samsung GT-I9000 Galaxy S установлена ОС Android версии 2.3, вы можете использовать программу Unlock Root. Список поддерживаемых программой устройств столь велик, что если его привести в книге, то он займет около 9 страниц! Конечно, публиковать такой огромный список я не стану, вы сможете скачать его по адресу:

http://dkws.org.ua/mybooks/android/unlock_root.txt

Программа одна, но последовательность действий может для каждого отдельно взятого телефона отличаться, поэтому прежде чем ее использовать, найдите в Интернете подробные инструкции именно для вашей модели.

Сейчас же мы рассмотрим, как использовать программу Unlock Root (рис. 10.7) для получения root-доступа на смартфоне Galaxy S с Android 2.3 на борту.

Итак, выполните следующие действия:

1. Включите режим отладки по USB (**Настройки | Приложения | Разработка | Отладка по USB**), также установите флажок **Приложения | Неизвестные источники**.

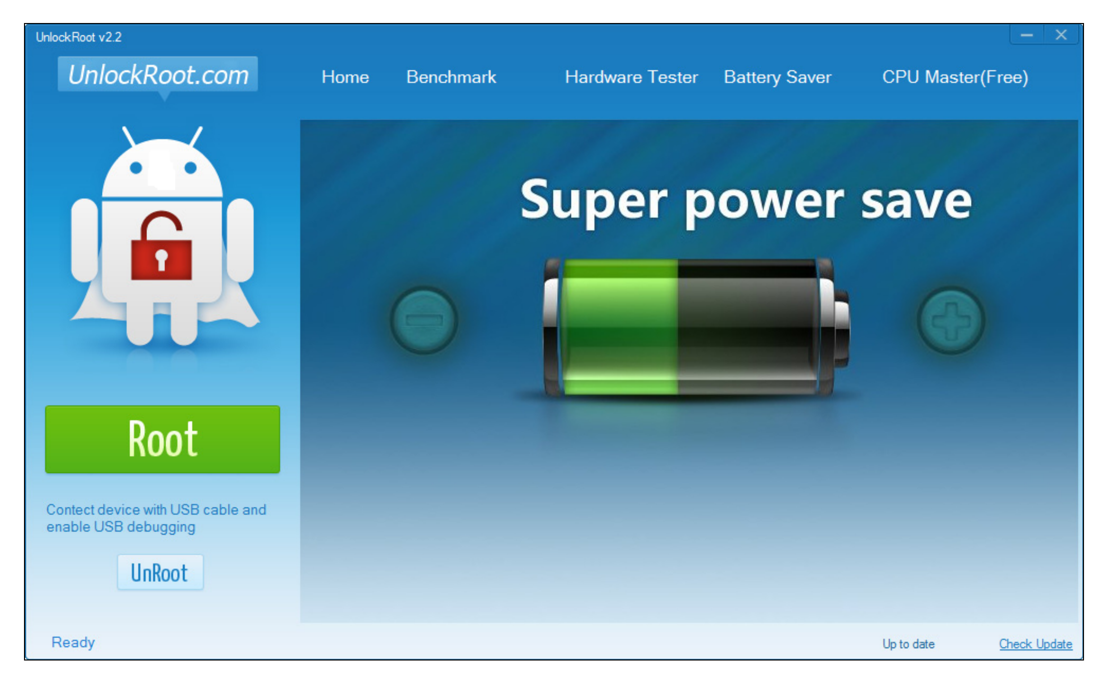


Рис. 10.7. Программа Unlock Root

2. Подключите USB-кабель к компьютеру.
3. Запустите программу Unlock Root.
4. Нажмите кнопку **Root**.
5. На вопрос программы, хотим ли мы перезагрузить устройство, ответьте нажатием кнопки **Да**.

Видеоинструкция по использованию программы Unlock Root доступна по адресу:

http://www.youtube.com/watch?v=6tm80wttTLY

Samsung GT-I9100 Galaxy S II

Сугубо теоретически вы можете использовать для получения root-доступа на этом смартфоне и программу Unlock Root, описанную в предыдущем разделе, но мы воспользуемся программой S2 Root, предназначенной именно для этого телефона.

Независимо от используемой для «разблокировки» телефона программы, прежде чем провести саму разблокировку, вам нужно с помощью программы Odin (рис. 10.8) установить так называемое *небезопасное ядро* Android, которое можно скачать по адресу:

http://forum.xda-developers.com/showthread.php?t=1101671

Еще раз о программах

Все необходимые для «рутования» программы, описанные в этой главе, можно найти в архиве по адресу: **http://www.dkws.org.ua/f/downloads**.

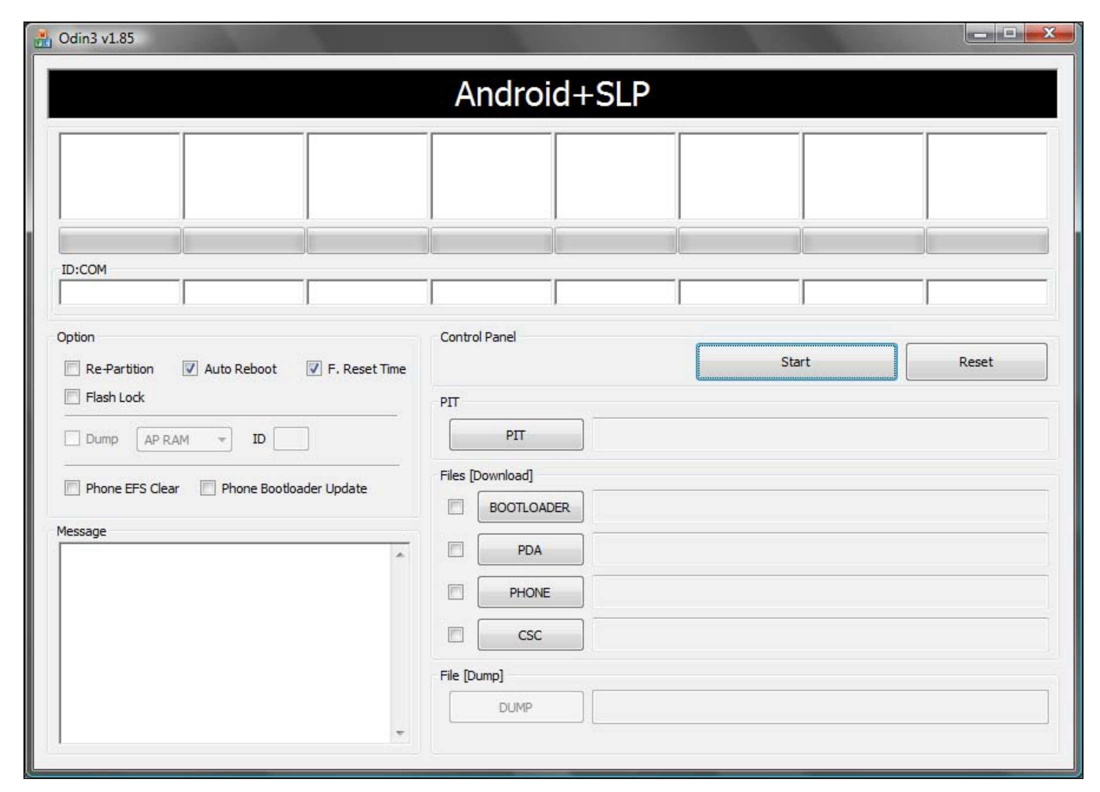


Рис. 10.8. Программа Odin

Небезопасные ядра я к себе на сайт не копировал, поскольку их много, и точно не известно, какое ядро понадобится именно вам. Но узнать это просто. Допустим, у вас смартфон GT-I9100. Введите комбинацию `*#1234#`. В графе **<SW VER>** вы увидите номер модели (**I9100**) и следом пять символов, которые означают версию программного обеспечения, — например, **XXKP1**. С этим «идете» на сайт, адрес которого указан чуть ранее, и качаете ядро именно для вашего смартфона.

Наверное, вам интересно, что означают эти пять символов номера прошивки? Первые две буквы — это страна, для которой сертифицирован телефон. Коды стран представлены в табл. 10.1.

***Таблица 10.1.** Код страны (прошивки Samsung)*

Код	Страна
AW	Венгрия
AZ	Франция
BD	Кипр, Греция
BY	Греция
CB	Польша
CE	Бенелюкс

Таблица 10.1 *(продолжение)*

Код	Страна
CP	Дания, Финляндия, Норвегия, Швеция
DB	Вьетнам
DC	Таиланд
DD	Индия
DT	Австралия
DX	Индонезия, Малайзия, Филиппины, Сингапур, Вьетнам
DZ	Малайзия, Сингапур
JA	Южная Африка
JC	Алжир, Марокко, Нигерия, Южная Африка, Тунис
JP	Арабский язык
JR	Арабский язык
JV	Алжир, Египет, Иран, Ирак, Кувейт, Марокко, Нигерия, Оман, Пакистан, Саудовская Аравия, Южная Африка, Сирия, Тунис, Турция
JW	Западная Африка
JX	Алжир, Египет, Иран, Ирак, Кувейт, Марокко, Нигерия, Оман, Пакистан, Саудовская Аравия, Южная Африка, Сирия, Тунис, Турция
KA	Турция
ME	Франция
MK	Сербия
MS	Франция, Германия, Италия, Нидерланды, Португалия, Испания, Турция, Соединенное Королевство
MT	Швейцария
MY	Италия
NH	Латвия
PO	Франция
RU	Россия
UB	Бразилия
XA	Австрия, Франция, Германия, Италия, Нидерланды, Швейцария, Соединенное Королевство
XB	Дания, Норвегия, Швеция
XC	Португалия, Испания
XD	Хорватия, Чехия, Венгрия, Словакия
XE	Болгария, Эстония, Казахстан, Латвия, Литва, Россия, Украина
XF	Болгария, Хорватия, Румыния

Таблица 10.1 *(окончание)*

Код	Страна
CP	Дания, Финляндия, Норвегия, Швеция
XP	Соединенное Королевство, Франция, Италия, Испания, Нидерланды, Польша, Португалия, Турция
XX	Австрия, Бельгия, Франция, Германия, Венгрия, Италия, Испания, Соединенное Королевство
XW	Австрия, Бельгия, Франция, Германия, Венгрия, Италия, Испания, Соединенное Королевство
ZC	Китай, Гонконг
ZH	Гонконг
ZS	Китай, Гонконг
ZT	Тайвань

После кода страны следует год выпуска телефона. L — 2012 год, K — 2011, J — 2010, ..., A — 2001.

Следующий символ — номер месяца выпуска телефона:

- A — январь;
- B — февраль;
- C — март;
- D — апрель;
- E — май;
- F — июнь;
- G — июль;
- H — август;
- I — сентябрь;
- J — октябрь;
- K — ноябрь;
- L — декабрь.

Последняя цифра — порядковый номер прошивки в этом месяце.

Итак, мы сделали небольшой перерыв. А теперь самое время вернуться к нашему процессу. Выполните следующие действия:

1. Включите отладку по USB (**Настройки | Приложения | Разработка | Отладка по USB**).
2. Перезагрузите смартфон в режим загрузки. Для этого выключите телефон и одновременно нажмите и удерживайте кнопки уменьшения громкости, <Home> и <Power>. Кнопку питания (<Power>) нужно нажать последней, иначе ничего не получится. Вполне возможно, что не получится и с первого раза. Если же вы все сделаете правильно, то увидите большой желтый треугольник по центру экрана с надписью **Downloading... Do not turn off target**.
3. Подключите смартфон к компьютеру и запустите программу Odin (для корректной работы этой программы нужен Samsung Kies, точнее драйверы, которые устанавливаются при установке Kies).

4. Выберите опции **Auto Reboot** и **F. Reset Time**, остальные должны быть выключенными (см. рис. 10.8).
5. Нажмите кнопку **PDA** и выберите ранее загруженное ядро.
6. Нажмите кнопку **Start** для замены ядра.
7. Подождите, пока устройство перезагрузится.
8. Если вы все сделали правильно, то во время загрузки устройства увидите желтый треугольник с восклицательным знаком. Это означает, что вы запускаете небезопасное ядро с вре́менными root-преимуществами.
9. Как только устройство загрузится, запустите на компьютере программу S2 Root (рис. 10.9) и нажмите кнопку **Root Device**. Если активен переключатель **Reboot Device When Finished**, устройство будет перезагружено по окончанию процесса.

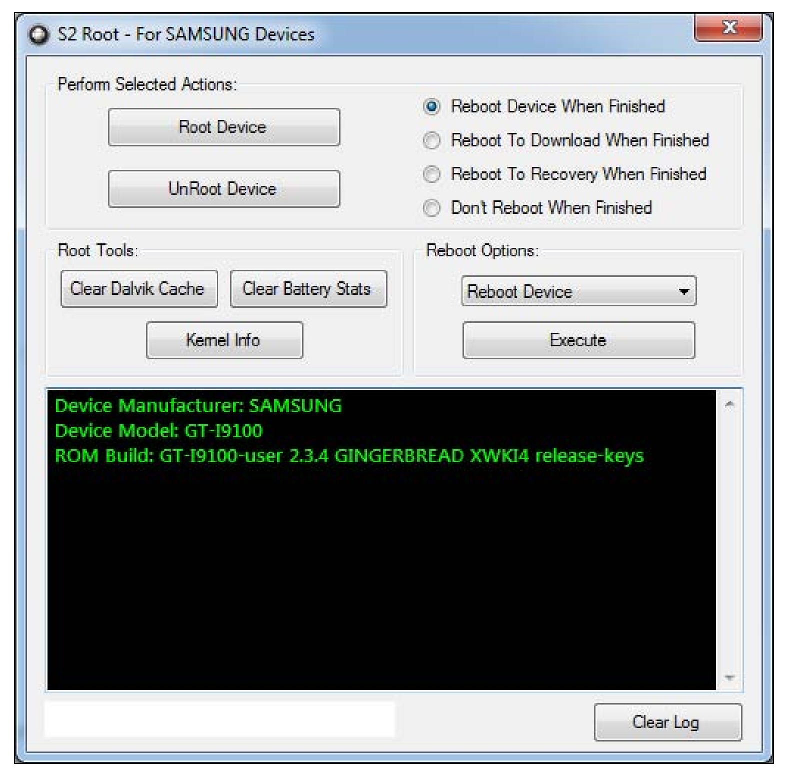


Рис. 10.9. Программа S2 Root

Примечание

Для работы программы S2 Root необходим Microsoft .NET Framework 4.0 или выше.

Побочный эффект этого способа — желтый треугольник при загрузке устройства. Он исчезнет после возвращения телефона на официальную прошивку (что нам пока не нужно), или его можно снять программой Triangle Away (Android 4.*x* ICS). Эту программу вы также найдете в том самом архиве, о котором шла речь в *разд. 10.2*.

Процедура использования программы проста до безобразия: установить и запустить программу, нажать кнопку **Reset flash counter**. У программы Triangle Away только один недостаток — она работает лишь на Android 4.0. На Android 2.3 вам придется использовать так называемый *джиг* — небольшое электронное устройство, которое нужно изготовить самостоятельно. «Рецепт» приготовления я нашел по адресу:

http://4pda.ru/forum/index.php?showtopic=246390&st=20#entry8067365

Однако сразу вас предупреждаю — лично я не тестировал этот способ и не могу гарантировать, что он рабочий. На мой взгляд, так в желтом треугольнике нет ничего страшного. А если придется обратиться в сервисный центр, тогда просто верните официальную прошивку, что можно сделать с помощью программы Samsung Kies, которая поставляется вместе с телефоном.

Впрочем, восстановить официальную прошивку поможет не только Samsung Kies, но и уже рассмотренная программа Odin:

http://androidp1.ru/odin-firmware-samsung/

10.3.3. Samsung GT-S5830 Galaxy Ace

Получить права root на этом устройстве можно с помощью все той же программы SuperOneClick. Включите режим отладки по USB, подключите телефон к компьютеру, но не включайте его в режиме монтирования карты памяти.

Далее последовательность действий практически такая же, как для других телефонов Samsung:

1. Запустите SuperOneClick, нажмите кнопку **Root**.
2. Если появится надпись **Waiting for device...**, отключите отладку по USB и снова включите ее. При необходимости повторите этот пункт, чтобы исчезла надпись **Waiting for device...**
3. Дождитесь завершения процесса.

10.3.4. Смартфоны HTC. Получение S-OFF

Со смартфонами Samsung и LG все было относительно просто — подключили телефон к компьютеру (и то не всегда, ведь в некоторых случаях можно было использовать GingerBreak и обойтись без компьютера), выполнили нужную последовательность действий — и права root «у вас в кармане». Только в редких случаях приходилось заменять ядро Android.

Со смартфонами HTC тоже будет несложно — если снять защиту, т. е. перевести телефон в так называемый режим S-OFF. Дело в том, что компания HTC внедрила в свои смартфоны последних поколений особую защиту — у системных разделов появился запрещающий в них запись флаг `@secuflag`. И при включенной защите (S-ON) для записи заблокированы разделы /system и /recovery. Кроме того, `secuflag` используется для проверки цифровой подписи при прошивке ZIP-файлов через опцию **Recovery**.

Для снятия защиты нам понадобится компьютер, способный загружаться с флешки (сейчас трудно найти компьютер, который не способен с нее загрузиться), а также чистая флешка.

Последовательность действий следующая:

1. Подключите флешку к компьютеру
2. Запустите программу unetbootin-windows-568.exe (рис. 10.10). Эта программа используется для записи ISO-образа на флешку, т. е. для создания загрузочного USB-диска.
3. Установите режим **Образ диска** и выберите флешку, на которую будет произведена запись.
4. Выберите ISO-образ alpharev.iso (и этот образ, и сама программа UNetbootin включены в состав архива необходимых программ, упомянутого в *разд. 10.2*).
5. Нажмите кнопку **OK** и дождитесь окончания записи.

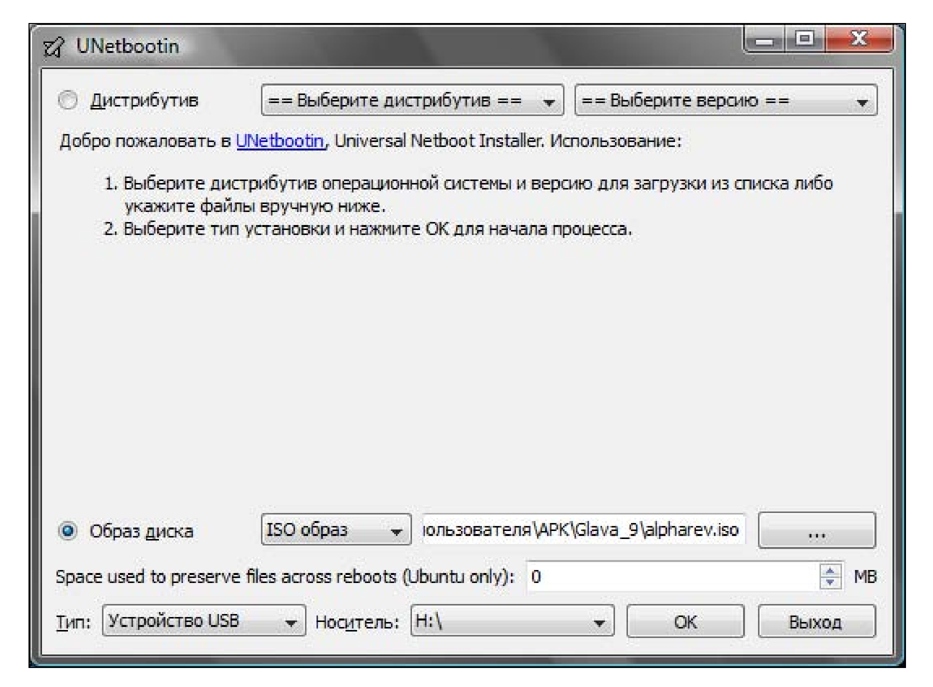


Рис. 10.10. Программа UNetbootin

6. Перезагрузите ваш компьютер и загрузитесь с только что созданной загрузочной флешки.
7. Запустится специальная программа, следуйте ее инструкциям. Когда будет нужно, подключите телефон к компьютеру и не отключайте его, пока не увидите сообщение об успехе. Ждать придется долго, по сообщениям некоторых пользователей — до одного часа. Если прошел час, а заветного сообщения вы так и не получили, отсоедините телефон, извлеките из него аккумулятор, вставьте его обратно и снова запустите описанную процедуру.

ПРОГРАММА REVOLUTIONARY

Это не единственный способ получить S-OFF на телефонах HTC. Есть еще программа Revolutionary, подходящая для всех моделей HTC. Подробную информацию об этой программе можно получить по адресу:

http://unrevoked.com/rootwiki/doku.php/public/revolutionary

А инструкция на русском языке по использованию программы Revolutionary находится по адресу:

http://4pda.ru/forum/index.php?showtopic=247336&st=0#entry7968420

Получив S-OFF, можно приступить к получению root-доступа. Существует несколько программ, позволяющих получить root-доступ на устройствах HTC. Я предпочитаю использовать современную программу Unlock Root. Она работает с большинством Android-устройств с версиями ОС Android от 2.1 до 4.0.3.

Последовательность действий следующая:

1. Отключите, а еще лучше — деинсталлируйте HTC Sync (если эта программа установлена на вашем компьютере).
2. Переключите устройство в режим отладки по USB (**Настройки | Приложения | Разработка | Отладка по USB**).
3. Подключите телефон к компьютеру.
4. Запустите программу Unlock Root.
5. Нажмите кнопку **Root**.
6. На вопрос программы, хотим ли мы перезагрузить устройство, ответьте нажатием кнопки **Да**.

В Интернете есть еще множество разных инструкций, позволяющих получить root на устройствах HTC. Вы без проблем найдете эти инструкции, если программа Unlock Root не поможет (хотя это маловероятно).

10.3.5. Sony Ericsson XPERIA Arc/Arc S

Получить root-доступ на Sony Ericsson XPERIA также можно с помощью программы Unlock Root. В скачанном вами архиве (см. *разд. 10.2*) имеются две версии этой программы: 2.3 и «старая». Для разблокировки Sony Ericsson XPERIA Arc/Arc S (рис. 10.11) следует использовать как раз старую версию.

Последовательность действий следующая:

1. Установите на компьютер все необходимые драйверы для смартфона (поставляются вместе с ним).
2. Установите программу Unlock Root и запустите ее.
3. Включите отладку по USB (**Меню | Настройки | Приложения | Разработка**), включите также установку из неизвестных источников (**Меню | Настройки | Приложения**).
4. Подключите телефон к компьютеру, на момент подключения телефон должен быть включенным.



Рис. 10.11. Смартфон Sony Ericsson XPERIA Arc

5. Как обычно, нажмите зеленую кнопку **Root**. Нужно немного подождать, пока программа сделает все необходимое.

После разблокировки программа предложит установить Battery Saver — лично я отказался от этой затеи, а просто перезагрузил смартфон (программа спросит, хотите ли вы сделать это — нужно согласиться).

После перезагрузки телефона вы обнаружите приложение Superuser (Суперпользователь), что означает, что вы получили права root.

10.3.6. ViewSonic ViewPad 7

Получить root-доступ на этом устройстве можно программой z4root, APK-файл которой вы найдете в загруженном архиве (см. *разд. 10.2*). Программа не требует установки на компьютер — это Android-приложение.

Установите программу на телефон и запустите ее. Далее все просто — нажимаем либо кнопку **Permanent Root** (если нужно получить root-доступ), либо **Un-root** (когда нужно вернуть все, как было).

Следует иметь в виду, что кнопка **Permanent Root** активирует постоянный root-доступ. После ее нажатия телефон перезагрузится, а вы получите права root. Можно также нажать кнопку **Temporary Root** — в этом случае телефон не будет перезагружен, а вы получите временный root-доступ, который «слетит» после перезагрузки телефона.

10.3.7. Acer Liquid S100

В загруженном архиве (см. *разд. 10.2*) имеется программа malezRecovery_0.6.1_Setup.exe. Она и используется для «рутования» устройства.

Перед началом процесса убедитесь, что установлены все драйверы и включен режим отладки по USB.

Подключите устройство к компьютеру и запустите программу malezRecovery. Она автоматически сделает все необходимое и перезагрузит телефон. Собственно, на этом весь процесс завершен.

10.4. Программа One Click Root

Программа One Click Root позволяет получить root-доступ на самых разных смартфонах и других Android-устройствах. Использовать программу очень просто:

1. Загрузите программу (**http://www.oneclickroot.com/download/**.
2. Подключите ваш смартфон к компьютеру.
3. Включите режим отладки по USB.
4. Запустите программу One Click Root и нажмите кнопку **Root Now**.

Вот список некоторых поддерживаемых моделей смартфонов:

- HTC Desire 200, Desire 500, Desire 600, Desire HD, Desire C, Desire X, One, One Dual;
- HUAWEI Ascend, Ascend G300, Ascend G330, Ascend G500 pro, Ascend G510, Ascend G600;
- LG Optimus 2X, Optimus 3D, Optimus 4X HD, LG Optimus F5/F7, Optimus L3, LG Optimus L3 II, Optimus L4 II, Optimus L5, LG Optimus L5 II, LG Optimus L9;
- Samsung Galaxy 5, Galaxy SL, Galaxy Tab, Galaxy Ace, Galaxy Core, Galaxy Note 2, Galaxy S, Galaxy S III, Galaxy S4.

Полный список всех поддерживаемых моделей приведен по адресу:

http://www.oneclickroot.com/phones/

10.5. Как узнать, что root-доступ получен?

Проще всего — попробовать выполнить действие, требующее прав root. Что именно? Вам лучше знать. Вы же получали root-доступ с определенной целью, а не просто так?

Вообще-то, после успешного получения root-доступа на устройстве должно появиться приложение Суперпользователь (рис. 10.12).

Теперь при запуске приложений, требующих полномочий root, вы увидите запрос, аналогичный показанному на рис. 10.13.

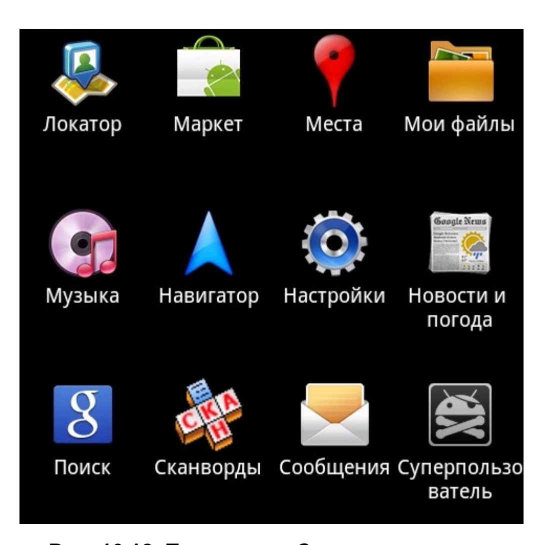


Рис. 10.12. Приложение Суперпользователь

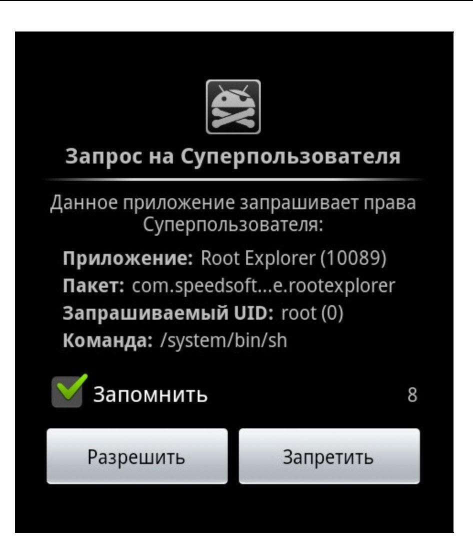


Рис. 10.13. Запуск программы, требующей root-полномочий

10.6. Активация отладки по USB в современных версиях Android

Для включения root-доступа требуется включить отладку по USB. До версии Android 4.1 (включительно) для этого достаточно было зайти в меню **Настройки | Для разработчиков** (или **Параметры разработчика** — в зависимости от версии Android), переместить переключатель в положение **ВКЛ**, после чего включить параметр **Отладка по USB** и нажать **OK**.

Однако, начиная с Android версии 4.2, пункт меню **Параметры разработчика** скрыт, и просто так включить отладку по USB уже нельзя. Чтобы открыть меню с параметрами для разработчиков перейдите в раздел меню **Настройки | О планшетном ПК** (или **Об устройстве** — смотря, какое у вас устройство: планшет или смартфон). Несколько раз нажмите на поле **Номер сборки** (рис. 10.14), после чего над полем появится сообщение **Шагов до включения режима разработчика**.

Нажмите на поле столько раз, сколько будет указано в этом сообщении, и откроется раздел **Параметры разработчика**, в котором можно включить параметр **Отладка по USB** (рис. 10.15).

10.7. Безопасный режим

В Windows и некоторых других операционных системах предусмотрен так называемый **Безопасный режим**. Аналогичный безопасный режим есть и в Android. Иногда смартфон под управлением Android начинает чутко тормозить. Вполне возможно, что «виноваты» сторонние приложения или виджеты. Но дело может быть и в самой системе. Чтобы выяснить это, нужно перейти в безопасный режим,

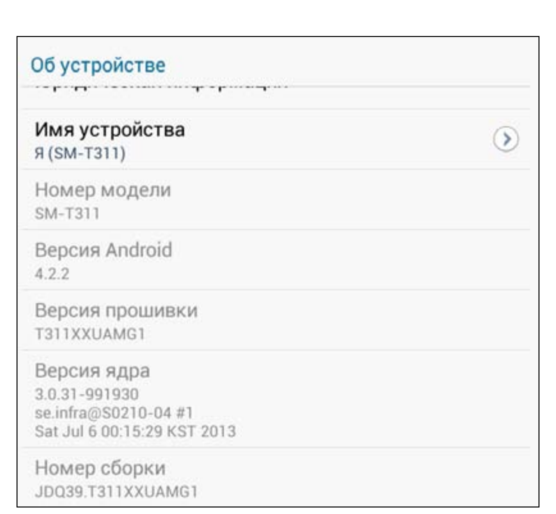



Рис. 10.14. Раздел **Об устройстве**

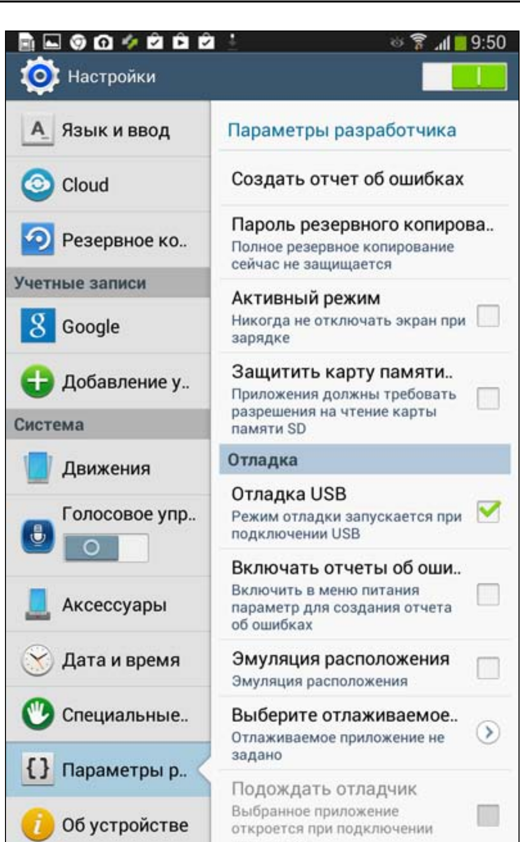


Рис. 10.15. Раздел **Параметры разработчика**

в котором не будут запущены различные сторонние приложения и виджеты. Если в безопасном режиме устройство нормально работает, вполне возможно, что причина в приложениях/виджетах, которые вы недавно установили. Попробуйте удалить недавно установленные приложения и запустите устройство в обычном режиме. Если это не помогло, поочередно удаляйте все сторонние приложения — так вы найдете «виновника». А уж после можно будет необходимые приложения установить заново.

Процедура перехода в безопасный режим различна для разных версий Android. Начиная с версии 4.1, перейти в безопасный режим можно так:

1. Нажмите и удерживайте кнопку выключения устройства. Появится меню завершения работы (рис. 10.16).
2. Нажмите и удерживайте кнопку **Отключить питание**, пока не появится приглашение перейти в безопасный режим (рис. 10.17).
3. Нажмите кнопку **OK**. Через пару секунд устройство будет выключено.
4. Снова включите устройство. Если вы все сделали правильно и устройство перешло в безопасный режим, то в нижнем левом углу вы увидите соответствующую надпись (рис. 10.18).

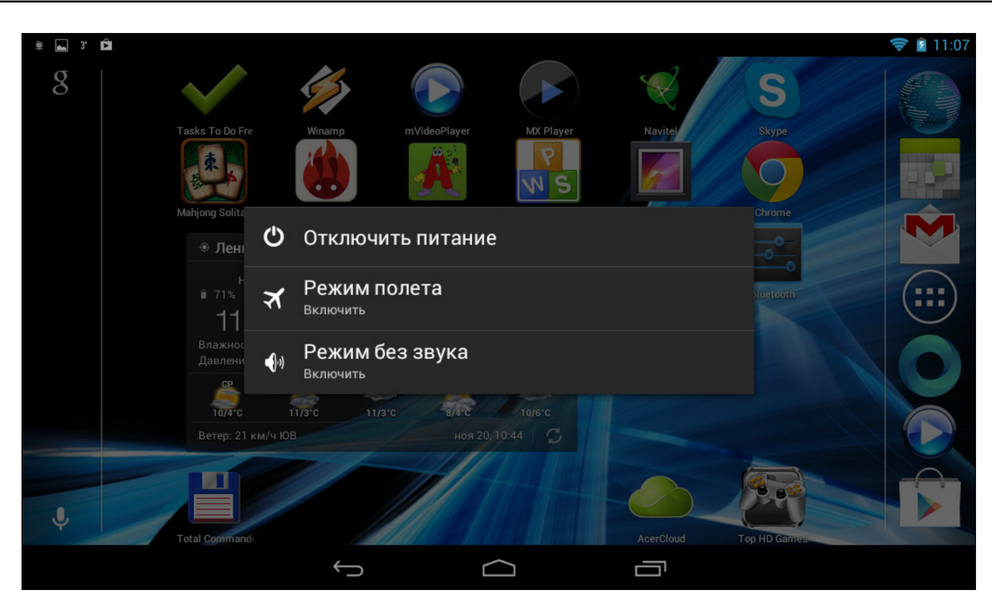


Рис. 10.16. Меню завершения работы

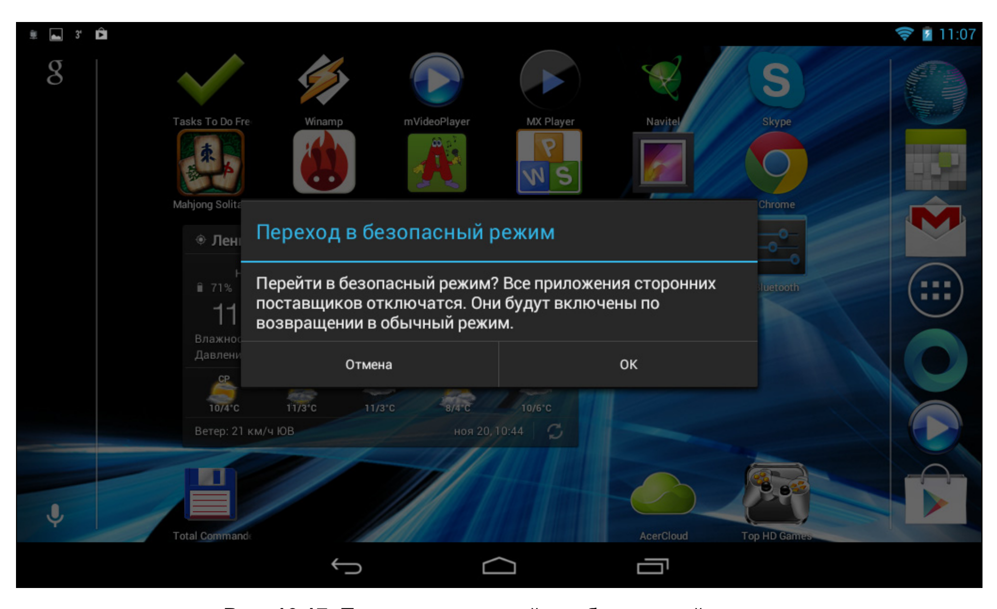


Рис. 10.17. Приглашение перейти в безопасный режим

5. Для выхода из безопасного режима нажмите и удерживайте кнопку выключения питания, в меню завершения работы выберите команду **Отключить питание** (кратковременно нажмите ее, удерживать не нужно). Устройство будет выключено. При следующем включении устройство будет загружено в обычном режиме.

В более ранних версиях (4.0 и ниже) переход в безопасный режим осуществляется иначе:

1. Выключите устройство.
2. Снова включите устройство, а как только увидите логотип при загрузке, одновременно нажмите кнопки повышения и понижения громкости и удерживайте их до тех пор, пока устройство не запустится. ОС будет запущена в безопасном режиме. Для выхода из него просто выключите и снова включите устройство.



Рис. 10.18. Устройство в безопасном режиме

10.8. Восстановление графического пароля

Некоторые Android-устройства поддерживают графические пароли. Суть их заключается в том, что пользователь выбирает рисунок, поверх которого «рисует» определенную траекторию. Устройство запоминает рисунок и траекторию, а при вводе пароля пользователь должен повторить эту траекторию поверх установленного рисунка, иначе устройство не разблокируется.

Так вот, если вы забыли, какую установили траекторию, или у вас не получается ее воспроизвести, чтобы разблокировать устройство выполните следующие действия:

1. Повторите ввод своего графического пароля пять раз. Не бойтесь, что будет превышено количество попыток ввода, — это как раз нам и нужно.
2. Вы увидите команду **Забыли графический ключ?** — выберите ее. Если она не появилась, через 30 секунд попробуйте снова пять раз ввести неправильный пароль и нажать кнопку **Домой** (Home). Команда должна появиться.
3. Теперь надо ввести адрес электронной почты и пароль от аккаунта Google. Конечно, до этого разблокируемое устройство должно быть подключено к Интернету — по Wi-Fi или через 3G (в этом случае на вашем счету у мобильного оператора должно иметься достаточно денег). Если адрес электронной почты и

пароль от аккаунта Google будут признаны правильными, устройство будет разблокировано, а вам предложат ввести новый графический пароль.

Однако этот способ подойдет не всем. Представьте, что у вас планшет типа Acer Iconia Tab, у которого нет 3G-модуля, а модуль Wi-Fi выключен, или рядом нет сети Wi-Fi, к которой ранее планшет подключался автоматически (для подключения к новой сети нужно, чтобы планшет был разблокирован). Нет соединения с Интернетом — значит, нельзя авторизоваться через Google, и способ не сработает.

Чтобы получить доступ к такому устройству, придется выполнить *аппаратный сброс*. Сразу предупреждаю, что в этом случае будут потеряны все данные (приложения, фотографии, электронная почта — словом, все), и устройство будет переведено в «заводское» состояние. Но так вы хотя бы сможете заново начать пользоваться своим устройством. А для сохранения хотя бы части данных извлеките внешнюю SD-карту. Если вы храните данные на ней, то они не пострадают. Конечно, если модуль Wi-Fi включен, проще перейти в зону действия сети Wi-Fi, к которой планшет подключался в последний раз — тогда он установит соединение с Интернетом, и можно будет попытаться сбросить пароль описанным только что способом.

К сожалению, процедура аппаратного сброса различна для разных моделей Android-устройств. Проще всего найти ее описание в Интернете по запросу: `*модель устройства* hard reset`.

Для аппаратного сброса некоторых моделей планшетов Samsung Galaxy Tab используется следующая процедура (в дальнейшем описании примем обозначение кнопки управления громкостью, которая находится ближе к кнопке включения устройства, — «–», а той, которая расположена дальше, — «+»).

1. Выключите устройство и нажмите кнопку включения и кнопку «–». Будет отображено сервис-меню, для смены команд в котором служит кнопка «–», а для выбора команды — кнопка «+». То есть, сначала с помощью кнопки «–» нужно выбрать нужную команду, а затем кнопкой «+» подтвердить выбор.
2. Выберите команду с изображением коробочки с зеленым роботом.
3. В отображенном списке действий нужно кнопками «–» и «+» выбрать действие: **wipe data/factory reset**.
4. Подтвердите желание выполнить аппаратный сброс, выбрав **Yes** в следующем списке. Будет выполнен аппаратный сброс, что занимает несколько секунд.
5. Выберите команду **reboot system now** для перезапуска системы. После перезапуска устройство будет готово к работе, и можно будет заново приступить к его настройке.

Еще раз напомню, что процедура сброса для других устройств Samsung может отличаться от описанной, и наверняка будет немного иной для устройств других производителей. Принцип, скорее всего, будет тот же, а вот кнопки, которые считаются «минусом» и «плюсом» могут оказаться другими.

ГЛАВА 11



Два телефона в одном

11.1. Концепция

Пока вы не приступили к чтению этой главы и не испортили свой смартфон окончательно, хочу вас предупредить. Если предыдущая глава называлась *На свой страх и риск*, то эту нужно было назвать *Для настоящих маньяков*. По сути, ничего рискованного в процедурах, описанных в *главе 10*, не было — как будет показано далее, получение root — не самая страшная операция, которую можно выполнить над смартфоном.

Еще раз повторюсь — вы должны понимать, что делаете. Эта глава для очень опытных пользователей Android, хорошо знакомых с ОС Linux (ядро Android — по сути, Linux) и владеющих навыками разработки Android-приложений. Перед тем, как «издеваться» над своим устройством, прочитайте всю эту главу до конца. Если вам что-то окажется непонятно, у вас есть два варианта: найти в Интернете объяснение (я не буду здесь описывать элементарные вещи) или же просто выбросить из головы эту затею и использовать описанные ранее способы защиты данных. Если вы сомневаетесь в своих умениях и навыках, лучше попросите кого-то более опытного вам помочь. Настоятельно рекомендую купить для экспериментов какой-нибудь недорогой, бывший в употреблении смартфон. На барахолках и на досках объявлений в Интернете такие смартфоны продаются очень дешево. И не беда, что, может, его аккумулятор «держит» не очень долго или весь экран поцарапан. Для нас важно не это — главное, чтобы сам смартфон работал. Он послужит тем самым подопытным кроликом, которого принесут в жертву ради истины.

А теперь, собственно, сама концепция «двойного» телефона. Представьте, что на устройстве установлены две операционные системы: открытая и скрытая, зашифрованная. Первая служит для работы с несекретными, публичными данными. Если они попадут в руки злоумышленника, то он никак не сможет испортить вам жизнь, используя эти данные. Вторая, скрытая, операционная система предназначена для работы с зашифрованными данными. Шифроваться они будут «на лету», а храниться — на ext4-разделе, созданном на внутренней карте памяти смартфона. Понятно, что и храниться они там будут тоже в зашифрованном виде. Для переключения

в зашифрованный режим нужно будет выполнить специальный сценарий. Выход из зашифрованного режима также обеспечит отдельный сценарий. По сути, у нас получится смартфон «с двойным дном». Никто никогда не заподозрит, что на устройстве установлена дополнительная операционная система.

11.2. От чего мы защищаемся?

На многих Android-устройствах очень легко можно получить root-доступ. Следовательно, если такой смартфон попадет в руки злоумышленника, тот сможет получить доступ к любым данным. Некоторые устройства вообще продаются уже с установленным root-доступом, да к тому же со скрытой его индикацией, — другими словами, вы даже не будете знать, что на устройстве открыт root-доступ.

Как мы отмечали ранее, компания HTC, якобы для улучшения защиты собственных устройств, внедрила в них дополнительную «фишку» — S-OFF. Все бы хорошо, но у S-OFF имеется огромная дыра в безопасности — custom recovery (пользовательское восстановление). Это набор низкоуровневых утилит, используемых для сохранения и восстановления резервной копии всех разделов ROM устройства. Даже не хочется перечислять всего того, что можно сделать с помощью пользовательского восстановления. Злоумышленник может подменить ROM своей собственной прошивкой, после чего получит доступ к вашим данным.

Даже если на устройстве нет прав root, стоит PIN-lock, ADB выключен и включен режим S-ON, все равно имеются варианты доступа к хранящимся на нем данным. Например, для телефонов HTC разработано устройство XTC Clip[1], позволяющее перевести смартфон в режим S-OFF без потери данных, при этом даже не придется загружать операционную систему. Устройство позволяет загрузить смартфон в инженерном режиме и записать в него нужную прошивку. А после этого сделать со смартфоном и данными все, что захочется.

Получив к смартфону root-доступ, можно полностью скопировать каталог /data/, в котором находятся все пользовательские настройки: аккаунты, программы, параметры программ и т. д. Если скопировать этот каталог на смартфон такой же модели, мы получим клон исходного смартфона.

Интересно так же и следующее обстоятельство. В файле /data/system/accounts.db хранится база данных всех аккаунтов пользователя. Обычными средствами до нее не добраться, поэтому Google пожертвовал безопасностью и хранит все пароли в этой базе в открытом виде. А это означает, что, получив доступ к файлу /data/system/accounts.db, злоумышленник получит доступ ко всем вашим аккаунтам: Skype, Gmail и т. п. А зная ваши пароли, он на их основании может попытаться вычислить пароли, которые вы будете использовать в будущем. Для просмотра же файла /data/system/accounts.db нужно всего лишь установить программу типа sqlitebrowser.

[1] О том, как использовать XTC Clip, хорошо написано по этому адресу: **http://4pda.ru/forum/index.php?showtopic=233375**.

Кроме паролей, есть много других интересных баз данных — так, в файле /data/data/com.android.providers.telephony/databases/mmssms.db хранятся все ваши SMS и MMS, а в файле /data/data/com.android.providers.contacts/databases/contacts2.db — телефонная книга.

Да и вообще, когда есть права root, можно снять PIN-lock и пользоваться смартфоном в обычном режиме — зачем копировать отдельные базы данных, если можно получить к устройству полный доступ. Для этого нужно подключиться к телефону через ADB и ввести команды:

```
adb shell
# sqlite3 /data/data/com.android.providers.settings/databases/settings.db
sqlite> update secure set value=65536 where name='lockscreen.password_type';
sqlite> .exit
# exit
adb reboot
```

Первая команда вызывает ADB-оболочку, вторая — вызывает утилиту sqlite3 (если sqlite3 отсутствует, ее нужно скачать отдельно и «прошить» через ADB), третья — это уже команда `sqlite3`, т. е. SQL-оператор. Четвертая команда — выход из sqlite3, далее выход из оболочки (команда `exit`) и последняя команда перезагружает смартфон.

Как защититься от всего этого? Есть два основных способа. Первый — не покупать телефоны, к которым можно получить root-доступ и включить режим S-OFF (в случае с HTC). Второй — шифроваться. Первый способ не дает никаких гарантий, что завтра не будет найден способ получения root для вашего аппарата. Второй же способ значительно более универсальный. Конечно, можно использовать встроенное шифрование, как описано в *главе 4*, можно шифровать отдельные данные (но телефонная книга, SMS и MMS останутся открытыми), а можно пойти по пути «максимального сопротивления» и создать еще одну зашифрованную операционную систему внутри смартфона, чем, собственно, мы здесь и займемся далее.

11.3. Реализация идеи

Наступил момент истины — мы подошли к самой сложной части этой главы. Еще раз напоминаю, что все действия нужно производить на «подопытном» смартфоне. Желательно, чтобы «подопытный» смартфон был бы той же модели, что и ваш основной, чтобы не получилась ситуация, когда «подопытный» выжил, а основной смартфон — нет.

Все описанное далее должно работать на операционных системах Android версий 2.3–4.1. Возможности проверить более новые устройства (с версией 4.2) у меня не было, но, учитывая «навороченность» версии 4.2, скорее всего, с самыми новыми устройствами, приведенный здесь способ потребует модификации или вообще не сработает.

Итак, для продолжения нам потребуется смартфон с Android версий 2.3–4.1, а также некоторая его подготовка. Прежде всего, нужно получить root-доступ (о том, как это сделать, было рассказано в *главе 10*).

Затем установить на смартфон:

- busybox — пакет консольных утилит;
- lm.cryptsetup — менеджер криптоконтейнеров.

Надо также включить USB-отладку и заполучить бинарник reboot из ROM Manager. Все необходимое программное обеспечение можно заполучить на форуме **http://4pda.ru/**. При некотором везении можно даже найти какую-нибудь прошивку (ROM), в которой уже есть все необходимое. Например, для HTC Desire можно использовать прошивку Leedroid Rom.

Во многих устройствах размер внутренней оперативной памяти (не путать с размером внутренней памяти устройства, используемой для данных, — назовем ее здесь для удобства внутренней SD-картой) равен 1 Гбайт. Поэтому предлагаю поделить этот объем пополам: 500 Мбайт — для зашифрованной системы и 500 Мбайт — для открытой. Сказано — сделано:

```
#busybox dd if=/dev/zero of=/data/crypt0 bs=1M count 500
#losetup /dev/block/loop3 /data/crypt0
#lm.cryptsetup luksFormat -c aes-plain /dev/block/loop3
```

Первая команда создает файл /data/crypt0 размером 500 Мбайт, вторая — привязывает его к loopback-устройству, а третья — форматирует этот файл, используя 128-битное AES-шифрование.

Итак, наш контейнер для дальнейшей работы уже создан. Открываем его и форматируем под файловую систему ext4:

```
#lm.cryptsetup luksOpen /dev/block/loop3 data
#mke2fs -T ext4 -L crypt0 -F /dev/mapper/data
#lm.cryptsetup luksClose  data
```

Первая команда открывает контейнер, вторая форматирует его, третья — закрывает.

Теперь займемся внутренней SD-картой. Нам нужно разбить ее на две части: одна будет использоваться для открытой операционной системы, вторая — для закрытой. Чтобы разбить карту памяти, мы воспользуемся утилитой parted (она есть в меню custom recovery, а если вы не знаете, как получить к ней доступ, найдите в Интернете инструкции для вашего смартфона):

```
parted /dev/block/mmcblk1
rm 1
mkpartfs primary fat32 0 4032
mkpartfs primary ext2 4032 8065
quit
```

Не спешите вводить все эти команды подряд. Первая команда вводится в приглашении оболочки, а остальные — в приглашении утилиты parted. Команда `rm 1` удаляет единственный раздел на SD-карте. Имейте в виду, что с ним будут удалены и все имеющиеся там в настоящий момент данные!

Следующие две команды считают, что размер внутренней SD-карты — 8 Гбайт, поэтому они делят ее поровну. Если в вашем смартфоне другой размер SD-карты, измените параметры, задающие размеры разделов.

Последняя команда выходит из parted. В результате на внутренней SD-карте должно появиться два раздела: /dev/block/mmcblk1p1 и /dev/block/mmcblk1p2. Первый раздел будет виден при подключении смартфона к компьютеру по USB. Второй раздел не будет виден вообще. Правда, его увидит Linux, если подключить смартфон к компьютеру под управлением этой ОС. Но при подключении к Windows все будет выглядеть так, как будто в смартфоне внутренняя карта памяти имеет 4 Гбайт вместо 8-ми, что часто бывает в некоторых моделях. Не думаю, что кто-то станет копать глубже.

Теперь у нас есть блочное устройство, и loopback-устройство уже больше не нужно. Отформатируем раздел в Luks:

```
#lm.cryptsetup luksFormat –c aes-plain /dev/block/mmcblk1p2
```

Откроем созданный контейнер SD-карты:

```
#lm.cryptsetup luksOpen /dev/block/mmcblk1p2 sdcard
```

После этого отформатируем открытый контейнер в FAT32:

```
#mkfs.vfat -n Seccard0 /dev/mapper/sdcard
```

Осталось только закрыть контейнер SD-карты. После закрытия о нем можно будет забыть на некоторое время:

```
#lm.cryptsetup luksClose sdcard
```

Главное сейчас — заполнить открытый контейнер данными. В настоящий момент он пуст, а поэтому наша зашифрованная система работать не будет. Сначала откроем его:

```
#losetup /dev/block/loop3 /data/crypt0
#lm.cryptsetup luksOpen /dev/block/loop3 data
```

Затем перемонтируем наш контейнер в режиме `rw`, создадим в корне папку /crypt_data и подмонтируем к ней наш зашифрованный контейнер:

```
#mount –o remount,rw /
#mkdir /crypt_data
#mount –t ext4 /dev/mapper/data /crypt_data
```

Теперь нужно скопировать из исходной папки /data в папку /crypt_data все, кроме ../dalvik-cache/ (кэш будет создан при первом запуске зашифрованной системы) и ../d (и, конечно, без файла crypt0 «весом» 500 Мбайт):

```
# cp -a /data/app /crypt_data
# cp -a /data/app-private /crypt_data
# cp -a /data/backup /crypt_data
# cp -a /data/data /crypt_data
# cp -a /data/dontpanic /crypt_data
# cp -a /data/drm /crypt_data
```

```
# cp -a /data/etc /crypt_data
# cp -a /data/htcfs /crypt_data
# cp -a /data/local /crypt_data
# cp -a /data/misc /crypt_data
# cp -a /data/property /crypt_data
# cp -a /data/secure /crypt_data
# cp -a /data/system /crypt_data
# cp -a /data/zipalign.log /crypt_data
# mkdir /crypt_data/d
# mkdir /crypt_data/dalvik-cache
```

Мы существенно продвинулись — у нас уже есть дубль нашей системы со всеми данными. Поэтому закроем контейнер:

```
# umount /crypt_data
# lm.cryptsetup luksClose data
```

В результате мы имеем два подготовленных контейнера, и осталось придумать способ, которым можно загружать и выгружать зашифрованную операционную систему «на лету», т. е. без перезагрузки смартфона. Кроме того, нам нужно заменить содержимое каталогов /data и /mnt/sdcard содержимым заранее подготовленных зашифрованных контейнеров, а также предусмотреть способ возврата обратно без потери данных и без перезагрузки смартфона.

Решение, предлагаемое здесь, не отличается утонченностью, но при желании вы можете создать собственное решение («по образу и подобию»), которое вам будет нравиться больше.

```
# sync
# setprop ctl.stop zygote
# mount -o remount,rw rootfs /
# mkdir /crypt_data
# mkdir /mnt/crypt_SD
# mount -o move /mnt/sdcard /mnt/crypt_SD
# lm.cryptsetup luksOpen /dev/block/mmcblk1p2 sdcard
# mount -t vfat /dev/mapper/sdcard /mnt/sdcard
# mount -o remount,ro rootfs /
# mount /dev/block/mmcblk0p26 /crypt_data
# losetup /dev/block/loop5 /crypt_data/crypt0
# lm.cryptsetup luksOpen /dev/block/loop5 data
# umount /data -l
# mount -t ext4 /dev/mapper/data /data
# setprop ctl.start zygote
# killall zygote
```

Решение, повторюсь, грубоватое, и при желании вы можете его изменить. В данном случае алгоритм прост. Сначала мы на всякий случай останавливаем процесс `zygote` (как известно, при старте системы Android запускает этот процесс, который порождает новые экземпляры Dalvik VM — по одному для каждого приложения), а после выполнения подмены папок /data и /mnt/sdcard — опять запускаем этот процесс. По-

сле чего командой `killall zygote` мы, по сути, перезапускаем Android без физической перезагрузки устройства.

В самой подмене каталогов нет ничего сложного, и написать такой сценарий может любой пользователь Linux. Да, совсем забыл — оформите все эти команды в виде сценария, чтобы их не пришлось вводить при каждом входе в защищенную операционную систему.

После последней команды (`killall`) вы окажетесь в зашифрованном режиме, который внешне похож на обычный режим, как две капли воды. И чтобы не путаться в режимах, как-нибудь измените его внешний вид — например, поменяйте обои.

Работа в зашифрованном режиме ничем не отличается от работы в обычном. Вам доступны все функции смартфона в полном объеме, а потери в производительности настолько ничтожны, что на них можно не обращать внимания.

Все бы хорошо, но теперь нужно придумать способ «вернуть все, как было», т. е. переключения в обычный режим. Стандартные операции включения/выключения не подойдут — вы повредите данные, и смартфон может вообще перестать загружаться.

Выполним следующий сценарий:

```
#sync
#setprop ctl.stop zygote
#setprop ctl.stop runtime
#setprop ctl.stop keystore
#fuser /data -m -k
#umount /data
#/lm.cryptsetup luksClose data
#/system/bin/reboot
```

Первая команда, как и в предыдущем случае, служит для синхронизации всех буферов ввода/вывода с носителем данных. Далее, останавливаем процесс `zygote`, останавливаем также процессы `runtime` и `keystore`, размонтируем каталог /data и отправляем устройство в перезагрузку командой `reboot`.

Вот и все. Теперь у нас есть смартфон с двумя операционными системами Android, которые можно загружать по требованию. Идеальный вариант для Джеймса Бонда — два телефона в одном. Главное, что никто ничего не заподозрит.

Как использовать такое устройство — решайте сами. Можно зашифрованную ОС предназначить для хранения деловых данных, а открытую — личных, или наоборот. Можно просто использовать их как различные операционные системы — например, если у вас два рода деятельности. В одной операционной системе хранить одни контакты, в другой — другие. При этом ни контакты, ни SMS, ни какие-либо другие данные не перемешаются между собой, а шифрование будет дополнительным бонусом. Сценариев применения достаточно много, думаю, каждый найдет нужный для себя.

Впрочем, в варианте «разведения» контактов по разным ОС кроется и некоторая сложность. Представьте ситуацию: вы решили использовать открытую ОС для ра-

боты, зашифрованную — для личной жизни. В открытой хранятся контакты ваших коллег, в закрытой — контакты ваших друзей и близких. На работе вы переключаетесь на открытую систему, после работы — на закрытую. Все хорошо, но есть ситуации, которые нам неподвластны. Например, в рабочее время приходит SMS/MMS от друга, жены, ребенка и т. д. Поскольку была активна открытая ОС, то полученное сообщение будет помещено в открытую часть системы, а этого бы вам не хотелось...

Поэтому, все же представленный здесь способ организации двойной загрузки больше подходит для хранения в телефоне чего-то секретного, что нужно скрыть от посторонних глаз, если телефон попадет в чужие руки.

Вместо заключения

Надеюсь, книга вам понравилась, и вы будете использовать на практике приведенные в ней рекомендации. Настоятельно рекомендую прочитать *приложение*, в котором описаны полезные (и не очень — чтобы вы их не устанавливали!) приложения, так или иначе связанные с мобильной безопасностью.

Если у вас возникнут вопросы, комментарии или просто пожелания, добро пожаловать на форум сайта **www.dkws.org.ua**. Всегда рад новым посетителям!

ПРИЛОЖЕНИЕ

Дополнительное программное обеспечение

Для Android разработано очень много приложений, так или иначе связанных с безопасностью: вашей личной, вашего имущества или ваших данных. В этом приложении представлено дополнительное программное обеспечение, не рассмотренное в книге, но с которым вы сможете разобраться самостоятельно, если возникнет такая необходимость. Во всяком случае, вы будете знать, для чего используется та или иначе программа, а установить ее уже — не проблема. Все описанные здесь программы можно найти на Google Play Маркет или скачать с сайтов их разработчиков. Все программы проверены мною лично, и вы узнаете не только об их преимуществах, но и о недостатках. Это тем более актуально, поскольку на Google Play Маркет, как правило, описываются только преимущества и функциональность программ, а об их недостатках можно узнать только после установки.

Безопасность данных и приложений

Safe+

Приложение Safe+ (рис. П1) позволяет хранить фото, видео, пароли и остальные данные в безопасности и недосягаемости для посторонних.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.zholdak.safeboxpro

Список часто задаваемых вопросов на сайте разработчика:

http://safebox.zholdak.com/faq/

XPrivacy

Приложение XPrivacy препятствует утечке персональных данных из программ, запущенных сервисов и т. д. Программа может также подменять ваши персональные данные по выбору — чтобы злоумышленник получил неправдивую информацию. У программы есть два недостатка. Первый — она требует права root. Второй — чтобы получить доступ ко всей функциональности, нужно купить PRO-версию за 4 или 6 долларов. Также для работы программы нужна Android 4.0 или более свежая версия.



Рис. П1. Приложение Safe+

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=biz.bokhorst.xprivacy.installer

> ***Важно!***
> Перед установкой программы XPrivacy сделайте резервную копию всех ваших данных!

Программу XPrivacy нельзя удалить, как любую другую. Для ее удаления следует воспользоваться специальной программой XPrivacy Remover, скачать которую можно по адресу:

http://4pda.ru/forum/index.php?showtopic=483684

Visidon AppLock

В *главе 4* была рассмотрена программа App Lock, позволяющая предотвратить запуск определенных приложений. Для запуска приложения нужно было ввести пароль: цифровой или графический. Есть более удобный способ идентификации пользователя — по его лицу. Для этого, конечно, нужно, чтобы смартфон был оснащен фронтальной камерой, но сегодня такие не редкость. Программа Visidon AppLock распознает пользователя по лицу и разрешает запуск защищенных приложений.

Однако помните, что программы такого рода легко обмануть, предоставив им вместо вашего реального лица его фотографию. Увы, пока не создана ни одна совершенная программа распознавания лиц. Может где-то такие и есть — например, в Пентагоне или ЦРУ, но уж точно не на Google Play.

Просмотреть это приложение в работе можно на YouTube:

https://www.youtube.com/watch?v=0FVWmeuj3T4

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=visidon.AppLock

LBE Security Master

Все пользователи Windows, думаю, знакомы с механизмом UAC (User Access Control, контроль учетных записей пользователей). В Android подобную функциональность реализует приложение LBE Security Master. Правда, в Windows все старались от UAC избавиться, а в Android пользователи в страхе перед «несчетным числом вирусов», наоборот, подобную программу устанавливают.

Нужно отметить, что в LBE Security Master уже встроен антивирус, поэтому если вы установите эту программу, то другой антивирус вам не понадобится, более того, установленный ранее антивирус наверняка будет конфликтовать с Security Master, поэтому вам придется выбирать: или ваш антивирус, или Security Master. Если вы выбрали Security Master, то имейте в виду, что кроме функций антивируса приложение умеет контролировать доступ приложений к Интернету, учитывать количество и устанавливать лимит интернет-трафика, блокировать рекламу в приложениях, создавать и управлять профилем энергопотребления, запускать приложения по расписанию, блокировать сообщения со спамом, очищать систему от файлов удаленных приложений и многое другое. Кроме того, приложение оснащено функцией Антивор, позволяющей отследить местонахождение вашего смартфона. Одним словом, полезная программа, заменяющая сразу несколько программ.

Однако есть у нее и недостатки. Во-первых, программа требует прав root. Правда, для некоторых устройств, которые программа «знает», она может самостоятельно выполнить «рутование», и вам не придется делать это «вручную». А во-вторых, приложение довольно сложное, но русского языка в его интерфейсе нет, поэтому пользователям, которые не знают английского, будет сложно разобраться со всеми его функциями.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.lbe.security

Официальный сайт:

http://www.lbesec.com/

KeepSMS

Приложение KeepSMS позволяет скрыть ваши SMS. Принцип работы его следующий — вы выбираете SMS, которые нужно скрыть, после этого для доступа к ним нужно будет ввести пин-код. Приложение умеет прятать цепочки SMS. Когда новое SMS из цепочки поступит на ваш телефон, оно будет сразу «спрятано» приложени-

ем, не будет и сигнала уведомления, а вы лишь увидите уведомление в строке состояния. Простое и удобное приложение.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.keepsafe.sms

Super Backup : SMS & Contacts

Программа для быстрого создания резервных копий/восстановления ваших контактов, сообщений и журнала звонков (рис. П2) позволяет хранить фото, видео, пароли и остальные данные в безопасности и недосягаемости для посторонних.

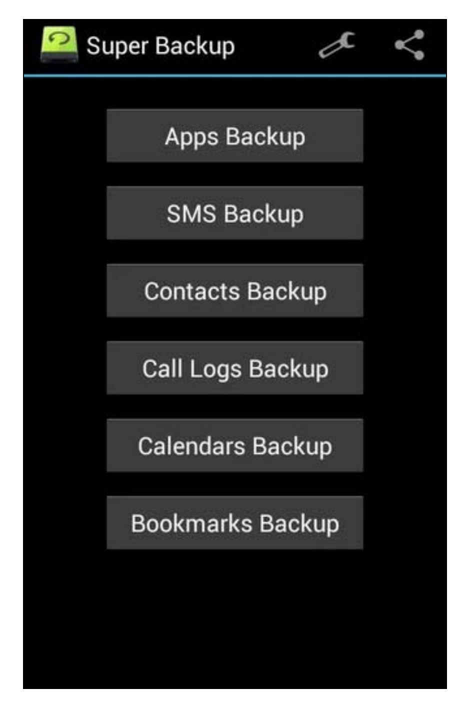


Рис. П2. Приложение Super Backup

Приложение очень просто использовать, и к тому же оно обладает русским интерфейсом.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.idea.backup.smscontacts

Поиск потерянного устройства

На Google Play можно найти много приложений для поиска потерянного или украденного устройства. В *главе 7* было представлено «родное» приложение от Google. Оно получилось очень удачным, но если оно чем-то вас не устраивает, вы можете рассмотреть и его аналоги.

Android Lost

Позволяет управлять вашим телефоном через Интернет или по SMS, а также позволяет обнаружить потерянное устройство.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.androidlost

> ***Предостережение***
>
> Программа Android Lost упомянута здесь, чтобы предостеречь вас от ее использования. На работу этой программы есть много жалоб, в том числе и на то, что она снимает деньги со счета. Однако свою функцию она выполняет и обнаружить потерянное устройство помогает. Использовать ее или нет — решать вам, но я бы присмотрелся к другим программам.

Cerberus

Приложение Cerberus (рис. П3) хорошее, но не без изъянов. Начнем с достоинств. Программа довольно функциональна и обладает русским интерфейсом. Вот неполный список ее возможностей:

- поиск и отслеживание телефона на карте;
- подача громкого сигнала тревоги, даже если телефон в беззвучном режиме;
- стирание памяти телефона и/или карты SD;

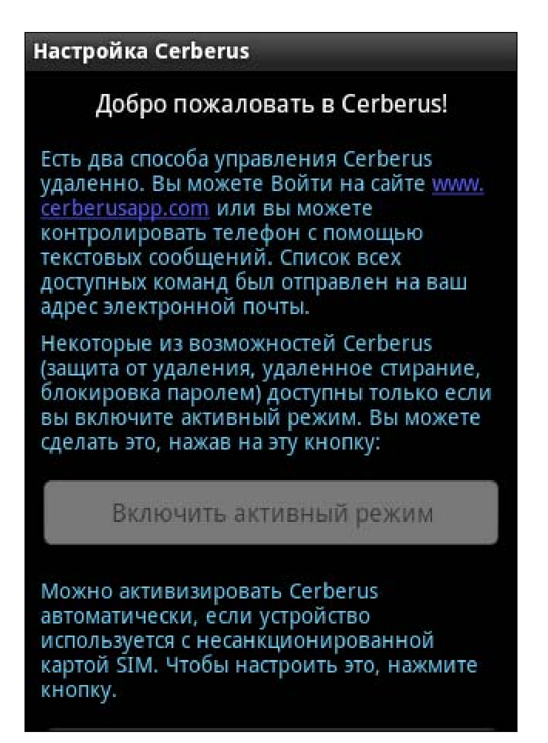


Рис. П3. Приложение Cerberus

- сокрытие из списка приложений;
- блокировка телефона секретным кодом;
- скрытая запись звука с микрофона;
- получение журнала последних переданных и принятых звонков;
- получение информации о сети и текущем операторе.

И это далеко не весь список. Хорошо, что программа умеет скрывать свое присутствие. Если вы скрыли программу, то для того, чтобы она опять появилась, наберите с помощью номеронабирателя `23723787`. После этого вы получите доступ к Cerberus.

> ***Внимание!***
>
> Согласно пользовательскому соглашению, разработчик приложения имеет право отключать и блокировать аккаунты с подозрительной активностью (использование приложения не по назначению, например, для мониторинга чужого телефона). Подозрительной активностью считаются частые запросы и многократная посылка команд через веб-интерфейс, в то время как в отслеживаемом аппарате установлена родная SIM-карта. Сколько именно команд можно отправить через веб-интерфейс, разработчик не сообщает, но уверяет, что для использования программы по прямому назначению, т. е. для поиска утерянного или украденного аппарата (предполагается, что злоумышленник установит в телефон свою SIM-карту), аккаунт не будет заблокирован. Другими словами, использовать данную программу в шпионских целях не получится. Если уж сильно хочется, тогда обратитесь к *разд. «Семейная безопасность»*, где представлены такие программы.

У программы есть и несколько недостатков:

- нестабильно работающий сайт — другими словами, если телефон «угнали», а сайт не работает, тогда отследить его местоположение вы не сможете;
- программа делает снимок «угонщика» и отправляет его на Google-аккаунт, при этом украденный смартфон тоже получит этот снимок (о чем сообщит в области уведомлений). В результате «угонщик» испугается — ведь теперь вам известно его лицо, и может даже уничтожить аппарат;
- программа платная — первые 7 дней ее можно использовать бесплатно, а потом — за деньги.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.lsdroid.cerberus

PhoneLocator Pro

Откровенно говоря — плохое приложение. На некоторых смартфонах работает, на некоторых — нет. На ряде устройств программа вообще не может включить GPS, а без него она мало чем полезна. Программу удалили с Google Play, но она все еще доступна на других сайтах с Android-приложениями. Не устанавливайте ее!

Хранение паролей

Last Pass

Программа Last Pass — отличный менеджер паролей и заполнитель форм. Запоминает ваши пароли и позволяет их автоматически указывать при необходимости. При этом программа хранит пароли в зашифрованном виде и умеет генерировать сложные пароли. Получается как бы два в одном: и генератор, и менеджер паролей.

Программа прекрасно работает, но у нее есть серьезный недостаток — она бесплатна только первые семь дней, а далее за ее использование придется платить $1 в месяц. Есть и еще один недостаток, кое для кого, может, и неважный, а для некоторых неприемлемый, — пароли программа хранит (хоть и в зашифрованном виде) на своем сервере. Это удобно, если вы поменяли телефон или используете программу на настольном компьютере (есть версии этой программы для Windows и Mac OS X). Достаточно ввести данные своего аккаунта на Last Pass, и вам будут доступны все свои пароли. Но одна мысль о том, что мои пароли хранятся на чужом сервере, заставляет волосы вставать дыбом. Это противоречит всем принципам безопасности.

Итак, вывод — программа справляется со своими функциями, но хранит ваши пароли на удаленном сервере. Использовать ее или нет — решать только вам. Если вы будете хранить в ней пароли для множества малозначимых ресурсов (типа форумов), то она может пригодиться, вот только стоит ли она $1 в месяц?

Ссылка на сайт разработчиков:

https://lastpass.com/

Dashlane Password Manager

Если вы постоянно имеете дело с паролями на разных ресурсах в Интернете, то программа Dashlane Password Manager — для вас настоящая находка. Существует две версии этой программы: Free и Premium. Бесплатная версия (Free) устроит большинство пользователей. Premium-версия отличается возможностью синхронизировать между собой несколько устройств. Если у вас один смартфон (планшет), то Premium-версия вам не нужна.

Программа содержит генератор паролей и функцию анализа ваших паролей. Если вы часто используете один и тот же пароль или же долго не меняли какой-либо пароль, программа предложит вам его сменить. Кроме ввода паролей программа позволяет заполнять и разные формы: логины, адреса e-mail, имена пользователя и т. п. Для шифрования паролей используется алгоритм AES-256.

К недостаткам программы можно отнести то, что она опять-таки хранит все ваши пароли на удаленном сервере. Если кто-то взломает этот сервер, то получит пароли всех пользователей, в том числе и ваши.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.dashlane#

eWallet Password Manager

eWallet — программа для хранения паролей, PIN-кодов, номеров кредитных карт в зашифрованном виде. В отличие от предыдущих программ, пароли хранятся на вашем устройстве, а не на удаленном сервере. Учитывая возможности программы, я бы ее назвал идеальным менеджером паролей, и она таким была, пока не стала платной. Не знаю, как вам, но мне ее цена не кажется приемлемой.

Если вы все-таки заинтересовались, вот ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.iliumsoft.android.ewallet.rw

Мобильные секреты

Приложение Мобильные секреты (рис. П4) умеет все то же самое, что и предыдущее (если не считать, что используется 128-битное, а не 256-битное AES-шифрование), но зато имеет бесплатную Lite-версию, которая хранит до 10 паролей. Если же вам этого покажется мало, тогда можно приобрести полную версию всего за 69 рублей — вполне нормальная цена за мобильное приложение.



Рис. П4. Мобильные секреты

Программа радует и ценой, и функциональностью, и интерфейсом. А главное — ваши пароли будут храниться только на вашем смартфоне, а не где-то еще. К тому же с сайта разработчиков вы можете скачать бесплатную версию (без всяких ограничений) для персонального компьютера под управлением Windows. Довольно заманчивое предложение, на мой взгляд.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.thefrogsoft.mobilesecretslite

Ссылка на сайт разработчиков:

http://www.thefrogsoft.com/

Safe In Cloud Password Manager

Еще один менеджер паролей, предлагающий хранить пароли в «облаке». Кардинальное его отличие от других подобных программ — то, что он в обычном режиме хранит пароли на локальном устройстве, но при желании вы можете синхронизировать их через «облако», причем не какое-то определенное, а по вашему выбору: Google Drive, Dropbox, OneDrive или Box — выбирайте то, которому больше доверяете. На телефоне же все пароли хранятся в зашифрованном виде с использованием 256-битного AES-шифрования.

Программа — платная, но ее стоимость не заоблачная, она более чем в два раза дешевле, чем eWallet.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.safeincloud

PassCreator

Каждый день взламываются тысячи аккаунтов в социальных сетях и на других сайтах. Причина — слабые пароли. Создать сложный для подбора пароль позволяют специальные программы — генераторы паролей.

Многие менеджеры паролей обладают функциями генератора паролей. Если вы выбрали менеджер без такой функции, то можете установить приложение PassCreator, которое сгенерирует сложный пароль.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.ddm.passcreator#

> ***Сложности запоминания***
>
> Сложные для подбора пароли являются также и сложными для запоминания. Не надейтесь на свою память, а лучше или запишите куда-то пароль, или воспользуйтесь менеджером паролей для его хранения.

Шифрование

Secure box

Приложение Secure box служит для шифрования файлов и хранения личных данных — таких как пароли, реквизиты кредитных карт и другие данные, которые лучше хранить в тайне. Для шифрования используются алгоритмы RSA и AES.

Приложение содержит набор шаблонов для данных, который может быть расширен пользователем. Обладает системой аудита действий, произведенных внутри приложений. Имеет встроенный менеджер резервных копий и способно шифровать файлы из приложений.

Secure box умеет работать с несколькими пользователями, что особенно актуально, когда устройство одно — например, домашний планшет, а пользователей несколько. Каждый пользователь приложения при этом видит только свои данные, а приложение исполняет роль администратора, который создает/удаляет учетные записи обычных пользователей.

Хотя на Google Play Маркет это приложение называется «Менеджер паролей», его возможности гораздо шире, чем просто управление паролями.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=ru.duke.securebox

Dark SMS

В *главе 6* было показано, как зашифровать сетевой трафик. Трафик-то мы зашифровали, но ведь SMS, которые вы отправляете и принимаете, видны мобильному оператору, поскольку передаются как обычный текст. А это не есть хорошо. Теперь для шифрования SMS вы можете использовать программу Dark SMS. По понятным причинам вы не найдете ее на Google Play. Я нашел эту программу во время работы над книгой на сайте **4pda.ru**:

http://4pda.ru/forum/dl/post/4449438/darksms.apk

Дополнительная ссылка на описание программы и комментарии установивших ее пользователей (кстати, на этом же форуме идут бурные обсуждения на тему законности применения этой программы и об ограничении длины ключа, чтобы программа соответствовала законодательству РФ, — очень рекомендую прочитать):

http://4pda.ru/forum/index.php?showtopic=558548

Для обмена зашифрованными SMS нужно, чтобы программу Dark SMS установили обе стороны: и отправитель SMS, и его получатель. Если вы отправите кому-то зашифрованное SMS, а у него не будет установлена программа Dark SMS, он не сможет его прочесть.

Cryptonite

Приложение Cryptonite обеспечивает шифрование данных на устройстве и в Dropbox и представляет собой бесплатную и открытую (OpenSource) реализацию шифрования файлов на основе EncFS (**http://www.arg0.net/encfs**).

Приложение будет работать не у всех. Во-первых, ему нужны права root. Во-вторых, требуется, чтобы ядро ОС поддерживало файловую систему в пространстве пользователя — FUSE (Filesystem in Userspace). Если ваш смартфон соответствует требованиям программы, вы получите мощные функции шифрования.

К сожалению, пользователей версии Android 4.2 не порадую, поскольку Cryptonite пока еще нестабильно работает на некоторых устройствах.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=csh.cryptonite

Crypt Haze

Приложение Crypt Haze использует 256-битное AES-шифрование для шифрования SMS-сообщений и электронной почты. Автоматически обнаруживает зашифрованные SMS. Программа вполне работоспособна, вот только кажется мне, что если она соответствует законодательству США и ее не удалили с Google Play Маркет, то не все так радужно, как кажется...

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=net.rehacktive.cryptdroid#

Crypto

Crypto — простая программа для шифрования текстовых сообщений. Обеспечивает RSA-шифрование и может быть использована больше для развлечения, чем в реальных целях. Вы можете зашифровать сообщение и отправить его своему другу, например, в чате или через систему личных сообщений в социальной сети. Друг, используя известный ему ключ (нужно еще позаботиться о том, чтобы безопасно передать сам ключ), может расшифровать сообщение и прочитать его.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=ru.mcprograms.crypto#

Семейная безопасность

Рассуждать на тему детей и компьютеров (разных, смартфон — тоже компьютер) можно бесконечно. Но ясно одно — детей от компьютера не оттянешь, поэтому нужно сделать работу максимально безопасной, как для ребенка (ограничив его от нежелательного контента), так и для самого компьютера (запретив запуск потенциально опасных приложений). Любой родитель также хочет знать, где находится его чадо в тот или иной момент времени. Поэтому семейной безопасности в этом приложении посвящен целый раздел.

Kids Place - With Child Lock

Программа Kids Place представляет собой детскую оболочку, неплохую оболочку с красивым детским интерфейсом. Она позволяет запускать лишь разрешенные приложения, чем спасет вас от потери данных и головной боли. Ребенок не сможет сделать звонок, отправить SMS, купить приложение.

Программа может работать в двух режимах: детском и родительском. В детском имеются ограничение запуска приложений (кроме разрешенных) и блокировка кнопки **Домой**. Всего на рабочий стол оболочки можно поместить до 48 программ — этого будет достаточно для даже самых требовательных детей.

Приложение бесплатное, но имеет платную PRO-версию, обладающую дополнительными функциями.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.whisperarts.kidsshell

Панель Родительского Контроля

Очень серьезное приложение для полного контроля детского телефона родителями. Родители могут использовать мобильный телефон ребенка в целях его же безопасности (ребенка, а не телефона!). При этом они имеют возможность:

- просматривать список установленных на мобильном телефоне ребенка приложений;
- запрещать запуск тех или иных приложений. Например, можно запретить запуск браузера, Play Market и т. д.;
- запретить изменение настроек телефона;
- видеть текущее состояние телефона — например, заряд аккумулятора и остаток памяти;
- контролировать текущее положение телефона ребенка, как с веб-сайта программы, так и со своего смартфона;
- получать уведомление от функции «Геозабор». Функция работает так — представим, что ребенок должен находиться на территории школы с 8 до 14 часов. Вы отмечаете территорию школы на карте. Если ребенок выйдет в указанное время за пределы этой территории, вы получите уведомление;
- получать от ребенка сигнал тревоги. Если ребенок попал в опасную ситуацию, он может или нажать специальную кнопку, или просто повернуть телефон три раза на 180 градусов. Этим он подаст сигнал тревоги своим родителям. После этого будет включен режим постоянного отслеживания положения устройства ребенка, и данные о местоположении устройства будут обновляться каждую минуту.

Если вы установили эту программу, то должны знать, как ее удалить. Просто так ее не удалишь. Зайдите в меню **Настройки | Безопасность | Администраторы**. Снимите флажок **Parental Board**. Теперь приложение можно удалить как обычно. Но если в меню пункта **Администраторы** нет, то удалить приложение удастся только путем отката до заводских параметров. Вы должны знать это перед установкой программы!

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.vionika.parentalBoard

Phone Control

Phone Control — довольно сложное приложение, но оно является настоящей мечтой родителя, поскольку обеспечивает полный контроль над телефоном ребенка, и работает при этом в скрытом режиме.

Неполный список возможностей программы:

- пересылка входящих/исходящих SMS/MMS на указанный в настройках мобильный номер или на адрес электронной почты;
- отправка уведомления о поступившем/исходящем звонке (номере абонента, времени звонка и продолжительности разговора) SMS-сообщением или на адрес электронной почты;
- получение отчета о географическом местонахождении телефона;
- запись телефонного разговора в аудиофайл, прикрепляемый к уведомлению о звонке (поддерживается пересылка только по электронной почте);
- пересылка фотографий и видео, сделанных с телефона (только по электронной почте);
- пересылка списка контактов телефона при помощи SMS с ключевыми словами;
- пересылка списка установленных приложений телефона при помощи SMS с ключевыми словами;
- пересылка закладок и истории посещаемых адресов при помощи SMS с ключевыми словами.

Несколько замечаний об использовании этой программы:

- установка ее на «целевой» телефон без согласия его владельца — нарушение закона и всех морально-этических норм. Надеюсь, вы это понимаете;
- у пользователя смартфона нет никаких значков этого приложения в списке приложений или области уведомления;
- чтобы получить доступ к приложению на «целевом» телефоне в номеронабирателе нужно набрать номер `74283` и нажать кнопку вызова. В настройках приложения можно изменить этот код;
- приложению *не* нужны права root.

На телефон родителя нужно установить программу Phone Control Admin, на телефон ребенка — программу Phone Control Key. Если у вас Android 3.1 или выше, то сначала нужно установить приложение Phone Control Enabler, а потом уже устанавливать приложение Phone Control.

Приложение довольно сложное и советую разобраться с инструкциями по его правильной установке и удалению. Подробные инструкции приведены по адресу:

http://4pda.ru/forum/index.php?showtopic=310081

По этому же адресу можно скачать и APK-файлы приложений (они также доступны и через Google Play Маркет).

Приложение Phone Control, хоть и немного сложное, но выполняет больше, чем от него ожидают и является лучшим в своей области. Для скрытой слежки — лучше приложения нет. Вот краткие характеристики аналогов:

- приложение MobileTool весьма напоминает Phone Control, но оно хуже. Во-первых, не столь богат функционал. Во-вторых, оно платное. В-третьих, требует root-доступа;
- функциональность приложения SMS Mobile Spy ограничена отслеживанием только SMS ребенка. К тому же приложение платное;
- то же касается и приложения Spy SMS Control. Оно хоть и бесплатное, но функциональность ограничена только SMS.

SmyleSafe: Parental Controls

Приложение SmyleSafe реализует родительский контроль веб-сайтов. Оно представляет собой безопасный детский браузер, способный заблокировать контент, который детям видеть нежелательно.

Использовать программу очень просто. Устанавливаете программу AppLock и запрещаете вызов Chrome и других браузеров, установленных на смартфоне, кроме браузера SmyleSafe. Другими словами, вы не даете ребенку права выбора — ребенок может запустить только браузер SmyleSafe, а уже он сделает свою работу очень хорошо.

К сожалению, приложение платное и за его использование придется заплатить $10.

Ссылка на сайт разработчиков:

http://www.smylesafe.com/

Сетевая безопасность

LostNet Firewall

В *главе 3* был рассмотрен очень удобный брандмауэр NoRoot Firewall. Кроме него существуют и другие брандмауэры, не требующие root-доступа. Один из таких брандмауэров — LostNet Firewall.

Приложение позволяет заблокировать доступ к Интернету любому приложению либо полностью, либо когда нет соединения Wi-Fi, что позволяет существенно сэкономить на трафике. А это одна из причин, по которой на смартфоны устанавливаются брандмауэры.

Также стоит отметить, что приложение полностью бесплатное.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.lostnet.fw.free#

Me Web Secure

Приложение Me Web Secure позволяет защитить смартфон от всякого рода неприятностей, с которыми можно столкнуться в Интернете, а именно — от спама, рекламы, вирусов и т. д.

Существует бесплатная (free) и платная (pro) версии этого приложения. Далее приводится ссылка именно на бесплатную версию:

https://play.google.com/store/apps/details?id=com.minaadib.mewebsecurefree

Личная безопасность и безопасность имущества

SOS APP

SOS APP — это простое приложение, которое может помочь сообщить вашим друзьям или родным, где вы находитесь и что с вами случилось. Приложение отправляет ваши координаты и голосовое сообщение на указанный заранее адрес электронной почты.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.reali.android.voicerecord#

Автосигнализация HipDriver

Приложение HipDriver позволяет организовать тревожную автомобильную сигнализацию на базе бюджетного смартфона, в том числе отслеживать снятие колес,

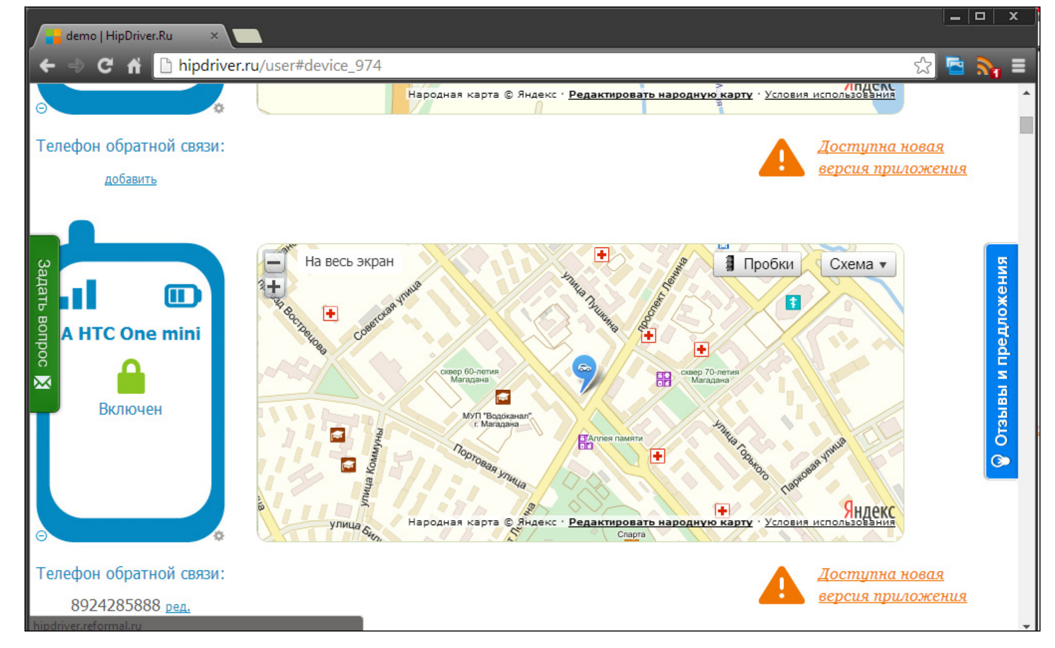


Рис. П5. Отслеживание положения машины

эвакуацию, удар и т. д., а также определять местоположение автомобиля в режиме тревоги (рис. П5).

Приложение не очень простое, подробную информацию по его использованию вы можете получить на сайте разработчиков:

http://hipdriver.ru/car_alarm

Бесплатна у приложения только Lite-версия, а за полнофункциональную нужно заплатить, но не очень дорого — всего 125 рублей.

Загрузить программу можно с Google Play Маркет:

https://play.google.com/store/apps/details?id=ru.hipdriver.android.app#

Gravity Alarm

Приложение Gravity Alarm (рис. П6) позволяет включить на смартфоне громкую сигнализацию на время вашего отсутствия и предотвратить тем самым использование его сторонними лицами. Вам нужно активировать программу — и ваш смартфон под охраной. Положите его на стол и можете спокойно выйти из кабинета — при перемещении смартфона вы услышите вой сирены. Идея неплохая, и само приложение интересное, но вы сами не сможете взять свой телефон без сирены. Поэтому такое поведение часто начинает раздражать. Лучше бы сирена срабатывала, если бы взявший в руки аппарат не смог, допустим, за 10 секунд ввести пароль (как это сделано в обычной сигнализации). Но, что есть, то есть.

Ссылка на Google Play Маркет:

https://play.google.com/store/apps/details?id=com.mgordey.gravityalarm#

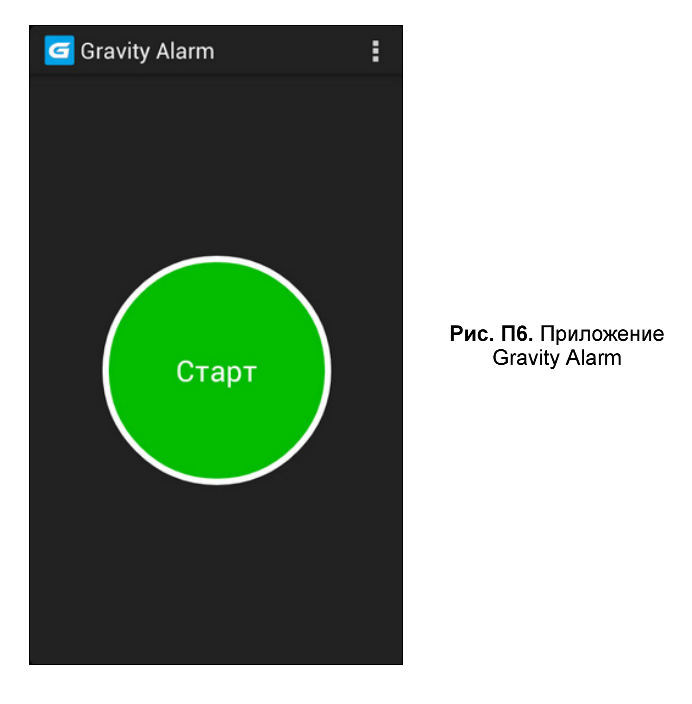


Рис. П6. Приложение Gravity Alarm

Предметный указатель

O

P

R

S

T







Z

А

Б

В

Д

З

К

М

Н

П

Р

С

Т



У

Ш